Information Operations Newsletter

Compiled by: **Mr. Jeff Harley**

US Army Space and Missile Defense Command
Army Forces Strategic Command
G39, Information Operations Division

The articles and information appearing herein are intended for educational and non-commercial purposes to promote discussion of research in the public interest. The views, opinions, and/or findings and recommendations contained in this summary are those of the original authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of the Army, or U.S. Army Strategic Command.

ARSTRAT IO Newsletter on Phi Beta Iota

ARSTRAT IO Newsletter at Joint Training Integration Group for Information Operations (JTIG-IO) - Information Operations (IO) Training Portal

Table of Contents

Vol. 12, no. 09 (July 2012)

Indian Navy Investigates Cyber Attack on Military PCs

From BBC, 4 July 2012

The Indian Navy is investigating a suspected hack attack.

A spokesman confirmed to the BBC that computers at its Eastern Naval Command had been infected with malware.

The announcement follows a report in The Indian Express saying that a virus had collected data from computers not linked to the internet and had sent it to IP addresses in China.

But security firm Sophos said it did not necessarily mean the hackers were based in China.

The Chinese Embassy in the UK did not provide comment.

The Eastern Naval Command has a security role on India's eastern borders, including protection of strategic and commercial assets.

It is reported that the information might have been collected via infected USB drives.

The malware is then thought to have created a secret folder on the drives where it stored documents, and as soon as the drive was plugged into a computer connected to the web, it sent the files to specific IP addresses.

Although those IP addresses were reportedly traced to China, an analyst from security firm Sophos warned against reading too much into the detail.

"Even if a hack is traced back to a Chinese IP address, it doesn't necessarily mean that Chinese hackers are behind the hack," Graham Cluley, senior technology consultant, told the BBC.

"It's very hard to prove who is behind an attack because hackers can hijack computers on the other side of the world and get them to do their dirty work for them. In fact, they often do this to cover their tracks.

"Finding the 'smoking gun' evidence of who was behind a particular internet attack is, for this reason, often very hard to find."

Table of Contents

China Hackers Enter Navy Computers, Plant Bug to Extract Sensitive Data

By Manu Pubby, Indian Express, New Delhi, Jul 01 2012

Hackers have broken into sensitive naval computer systems in and around Visakhapatnam, the headquarters of the Eastern Naval Command, and planted bugs that relayed confidential data to IP addresses in China.

The Eastern Naval Command plans operations and deployments in the South China Sea — the theatre of recent muscle-flexing by Beijing — and beyond. India’s first nuclear missile submarine, INS Arihant, is currently undergoing trials at the Command.

The extent of the loss is still being ascertained, and officials said it was “premature at this stage” to comment on the sensitivity of the compromised data. But the Navy has completed a Board of Inquiry (BoI) which is believed to have indicted at least six mid-level officers for procedural lapses that led to the security breach.

The naval computers were found infected with a virus that secretly collected and transmitted confidential files and documents to Chinese IP addresses. Strict disciplinary action against the indicted officers is imminent.

Responding to a questionnaire sent by The Sunday Express on whether highly classified data had been sent to IP addresses in China due to the bug, the Navy said: “An inquiry has been convened and findings of the report are awaited. It needs to be mentioned that there is a constant threat in the cyber domain from inimical hackers worldwide.”

Sources, however, confirmed that classified data had been leaked, and the breach had possibly occurred because of the use of pen drives that are prohibited in naval offices. The virus was found hidden in the pen drives that were being used to transfer data from standalone computers to other systems, said a person familiar with the investigation.

The Navy — and the other armed forces — stores sensitive data only in standalone computers that are not connected to the Internet. These computers are not supposed to have ports or access points for pen drives or external storage devices.

The virus apparently created a hidden folder and collected specific files and documents based on certain ‘key words’ that it has been programmed to identify.

The documents remained hidden on the pen drives until they were put in computers that were connected to the Internet, after which the bug quietly sent the files to specific IP addresses.

The cyber espionage came to light in January-February this year. Besides the Navy’s resources, other cyber forensic agencies were involved in tracing the hackers, sources said. China has been accused earlier of using “cyber battalions” — specially trained military staff — to break into sensitive computer systems across the world.

The Naval HQ in New Delhi is monitoring the case closely. Besides the Arihant trial, several other sensitive projects are being undertaken near Visakhapatnam, including an upcoming underground nuclear submarine base that is expected to house India’s strategic assets.

Table of Contents

Army Makes Case for Funding Culture Skills beyond COIN

By Sydney J. Freedberg Jr., AOL Defense, July 2, 2012

As budgets tighten and the wars wind down, the Army is struggling to institutionalize the hard-won cultural skills it learned in Afghanistan and Iraq -- and to make the case for their continued relevance and resourcing to an administration whose new strategic guidance swears off counterinsurgency.

Joint Chiefs Chairman Gen. Martin Dempsey himself recently touted the importance of "the science of human relationships" as essential far beyond Afghanistan. The Army, Dempsey's own service, has already begun to "align" specific brigades with specific regions they might operate, starting with Africa, so they can bone up on the local culture, language, and politics before they deploy, in an effort to replicate the pre-deployment training now done for Afghanistan for other parts of the world. But to secure funding for such efforts in the long term, the Army needs to enshrine them in joint doctrine.

At the heart of the Army's evolving argument is a concept so new it hasn't got an official name. "What we're working to avoid is getting trapped into a title," said Col. Robert Simpson of the Army's Training and Doctrine Command (TRADOC), in an interview with AOL Defense, though the leading proposed term is "human domain." What's essential, Simpson said, is "to make sure that we get into our doctrine, into our thinking in terms of the joint force and policymakers, that the purpose of any military operation is to affect human behavior." But current planning processes fixate on physical factors. What's necessary is a sophisticated cultural, sociological, and psychological understanding, he went on, of "what are our opponents wiling to fight and die for" -- and how to convince them to give up.

"It's not just COIN [counterinsurgency]," Simpson went on. "To take the extreme example, we dropped the atom bombs not to destroy Hiroshima and Nagasaki but to compel the Japanese people to surrender. That was purely a decision based on an intent to control behavior."

That may seem a cold-blooded way to talk about such lethal violence. It's uncontroversial nowadays to tout the importance of understanding and influencing foreign cultures in so-called "low-intensity" conflicts to "win hearts and minds." It's another matter to talk about high-intensity warfare as simply a way "to affect human behavior."

"To think of war as a bargaining process is uncongenial to some of us. Bargaining with violence smacks of extortion," wrote Thomas Schelling, one of the most influential political scientists of the Cold War, in his landmark 1966 book about superpower conflict in the shadow of nuclear weapons, Arms and Influence. "[But] coercion is the business of war."

Schelling was hardly the first to have this thought. It goes back to Carl von Clausewitz's dictum that "war is nothing but a continuation of political intercourse, with an admixture of other means" (often shortened to "war is politics by other means") and to Sun Tzu's admonition to "know your enemy and know yourself." But it's a new insight for the US military, whose closest approach to Sun Tzu has traditionally been to "know your enemy's technology and know your own."

Since Ulysses S. Grant in 1864, the mainstream American way of war has relied on concentrating superior firepower, logistics, and technology against enemy forces and grinding them down. That worked brilliantly in World War II, the 1991 Gulf War, and the 2003 invasion of Iraq; it worked less well in Korea and backfired disastrously in Vietnam. In Iraq and Afghanistan, the Army (and Marines) slowly learned to navigate a complex landscape of enemies, neutrals, and factions capable of changing from one to another, as in the famous "Anbar Awakening" movement where Sunni Arab insurgents turned against al-Qaeda.

Iraqi sheikhs and Afghan elders didn't have to read a political scientist like Schelling to know that violence can be negotiating tactic. But US military doctrine, planning, and budgeting processes fixate on the material aspects of war -- building weapons, locating targets, deploying forces, amassing supplies -- and not on whether all this effort would actually convince an enemy to give up, or better yet switch sides. That's something the Army now seeks to change.

"Over the last 12 years or so, [we] realized that we were not including the whole picture," said one Army officer who fought in Iraq. "Yeah, sometimes we had civilians on the battlefield," he said, "but we didn't deal with them in any professional manner: [We'd] throw MREs [rations] at these guys and make sure they have a tent, and then the kill the enemy army."

The Army is exploring how it might make use of civilians and neutrals in future "hybrid" conflicts that combine Taliban-style guerrilla fighters with nation-state-style weapons. The most recent annual wargame at the Army War College, for example, featured a new twist in the computer model. As simulated US and hostile forces hunted each other on the electronic map, their odds of spotting their opponent were affected by the political and ethnic leanings of local villages: A Muslim village helped militants detect US forces nearby, a Christian village helped the Americans.

During the wargame, senior officers and civilians convened to discuss the concepts it was testing, including the new emphasis on cultural factors. "Using human relations as an amplifier [for military operations] -- I found that really interesting," retired Maj. Gen. Robert Scales told AOL Defense afterwards. Scales has written on the need for cultural knowledge and argued social scientists will be as critical to future wars as nuclear physicists were to World War II, but, he said, "I had not seen this before" as a factor in Army wargames.

What to call this concept is an open question. Many in the Army advocate the term "human domain" -- which would explicitly and formally put it on par with the other "domains" officially enshrined in joint doctrine: air, sea, land, space, and cyberspace. "If we put it on par with the other domains we'll be forced to resource it, we'll be forced to train it," said one Army officer. Politically, however, convincing the other services to go along would be an uphill battle. Intellectually, separating out cultural and psychological factors as their own "domain" ignores how they are fundamental to all human conflict.

Whatever it's finally called, getting joint blessing for the importance of such human factors would help the Army make its case for funding in hard budgetary times. Better understanding of cultural, sociological, and psychological issues helps use materiel better, Simpson said -- it can't substitute for it. "We still need the equipment," he said. "We still have to dominate the physical environment as well." And that takes money that will be increasingly hard to get.

Table of Contents

Information as Power, vol 6

US Army War College, book link: http://www.csl.army.mil/InfoAsPower.aspx, May 2012

Preface: The U.S. Army War College (USAWC) is pleased to present this anthology of selected student work from Academic Year 2011 representing examples of well-written and in-depth analyses on the vital subject of Information as Power. This is the sixth volume of an effort that began in 2006. The anthology is an important component of an effort to coordinate and recommend the design, development and integration of content and courses related to the information element of power into the curriculum to prepare our students for senior leadership positions.

Interestingly, one needs to go back to the Reagan administration to find the most succinct and pointed mention of information as an element of power in formal government documents. Subsequent national security documents, to include the 2010 National Framework for Strategic Communication and the current National Security Strategy, allude to different aspects of information but without a holistic, overarching strategy or definition. Still, it is generally accepted in the United States government today that information is an element of national power along with diplomatic, military and economic power…and that information is woven through the other elements since their activities will have an informational impact. Given this dearth of official documentation, Drs. Dan Kuehl and Bob Nielson proffered the following definition of the information element: "Use of information content and technology as strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security." Information as power is wielded in a complex environment consisting of the physical, informational, and cognitive dimensions (alternatively referred to as "connectivity, content and cognition").

The current information environment has leveled the playing field for not only nation states, but non-state actors, multinational corporations and even individuals to cognitively affect strategic outcomes with minimal information infrastructure and little capital expenditure.

Anyone with a camera cell phone or personal digital device with Internet capability understands this. Adversary use of information as an asymmetric strategic means has been extremely effective in Iraq and

Afghanistan. On the other hand, the U.S. government and its military exploit the capabilities of cyberspace to communicate effectively, conduct daily business and plan and execute military operations. This capability, however, becomes a vulnerability of dependence that can be targeted by rogue individuals, criminals and adversary nation states. Clearly, managing the message while protecting the necessary technological means represent critical opportunities and challenges requiring risk analysis and mitigation.

U.S. strategic thought on these issues has advanced over the past six years as has the research and analysis of our students about these information-related topics. “Information as Power” is reflective of that intellectual evolution. We’ve moved from a discussion of what defines strategic communication in Volume 1 to the important but difficult process of measuring strategic communication effectiveness in this latest edition. We’ve shifted from a focus on network centric operations to future-focused strategic and operational analyses of cyberspace. As such, the anthology serves not only to showcase the efforts of the College but to inform the broader body of knowledge as the Nation advances its efforts to act proactively within this environment and to counter current and potentially future adversaries who so effectively exploit it.

Link: http://www.csl.army.mil/InfoAsPower.aspx

Table of Contents

At Nellis AFB, Teaching the Shadowy Art of Cyber Warfare

By Dave Toplikar, Las Vegas Sun (via Stars and Stripes), July 6, 2012

Flying above the clouds in hostile territory, a U.S. Air Force F-15E fighter pilot checks his computer to make sure he's on course, trying to steer clear of a no-fly zone.

But can he trust the information that comes up on his screen? Can he complete his mission without creating an international incident? Could a cyber terrorist network have hacked his data?

"How do you know you're clean? You don't. That's a continual problem that no one has solved," says the man in the shadows at Nellis Air Force Base, outside of Las Vegas.

As a jet engine roars from a nearby field, the man — who wants to be identified only as Steve because of the sensitivity of his work — ponders the hypothetical situation he has just described.

It's a scenario the quiet lieutenant colonel has been dealing with for the last few months: the world of cyber warfare.

"All you can do is protect yourself in the best way possible and continue to be vigilant to any indicators of adversarial activity," Steve said.

His eyes turn across the room to a colorful 3-D topographical wall map depicting the mountainous terrain and bleak desert landscape of the Nevada Test and Training Range.

Since 1949, military fighter pilots have been coming to the range to pass on the real-life lessons learned in past wars, including an upcoming Red Flag exercise this month in the 5,000 square miles of airspace.

But Steve operates on a different test range — one in the limitless virtual world of computer networks and communications systems.

He's the new director of operations of the Air Force's first Cyber Weapons Instructor Course.

Eight students recently graduated from the course after spending 10- to 12-hour days for six months going through a rigorous curriculum. The school's goal? To create leaders who can tackle problems as they arise with computer hackers.

Their coursework prepares them to teach others to recognize and learn how to deal with the possibility of a cyber attack. Graduates will become instructors and advisers to military leaders.

"We want our graduates to transform and inspire our nation's combat power, to bring the cyber piece to operational planning, but also to help build the cyber force to recognize that they are part of the overall picture and a capability we are providing to the combatant commander," Lt. Col. Bob Reeves, the commander of the 328th Weapons Squadron at Nellis, said in a prepared statement.

The Air Force has been charged with protecting its own communications networks in the virtual domain, which is the mission that drives the Cyber Weapons Instructor Course, Steve said.

"Our adversaries will be using this domain to come after us," Steve said, "and we want to maintain the ability to protect against them."

The instructors in his program will go on to work with the Department of Defense's Cyber Command, which also draws forces from the Army, Navy and Marines, Steve said.

So far, the military hasn't seen any serious outside threat that has actually broken into the Air Force's operations. But it could happen, he said.

"Right now, it's entirely plausible for someone to use computer networks as a means to collect intelligence, and that's what we see on a daily basis as the biggest threat we're responding to today," he said. "We're preventing people from collecting that intelligence."

Threats come from individual hackers or from cyber guerrillas hired by countries hostile to U.S. interests, he said.

There are also "hacktivist" groups, such as the loose-knit "Anonymous" collective. Last year, Forbes reported Anonymous was seeking to disrupt communications at the Quantico, Va., base where Pfc. Bradley Manning was incarcerated on charges he had given documents to WikiLeaks.

Steve said the National Security Agency is charged with warning when it sees cyber intrusions.

The Department of Homeland Security is probably the most likely target of any cyber attack, he said. Other likely targets are the military branches, energy companies, cable companies or the banking system, he said.

Are home computers susceptible to hackers?

"It's unlikely they would find a normal individual a high enough payoff to go through the effort of impacting them," Steve said. "But could they? Yes."

Before coming to the Cyber Weapons Instructor Course at Nellis, students go through three months of Undergraduate Cyber Training at Keesler Air Force Base, Miss., and two months of Intermediate Network Warfare Training at Hurlburt Field, Fla.

Most of the original eight students came from the 67th Network Warfare Wing and 688th Information Operations Wing at Lackland Air Force Base in San Antonio, Texas.

The main goal of the program is to help them recognize if a problem has occurred, figure out what went wrong and go about fixing it, Steve said.

"It's a problem-solving mindset," he said.

As part of Nellis' Warfare Center, aircraft use the Nevada Test and Training Range to simulate warfare scenarios.

"We have a virtual world out there on the computer side that's the counterpart to that," Steve said.

They use an "aggressor squadron" that attacks from both the aircraft side of the training and from the information side, he said.

"They do what they can to emulate what a bad guy would do, or a thinking adversary," Steve said. "So they challenge our students with a different problem set every time. We take some liberties with what the adversary's capabilities are to change the scenarios for the students."

Real-world scenarios are put together for students, he said.

"We pick a region of the world where there would be increasing tensions and an adversary who doesn't want U.S. involvement in that area — typically where a no-fly zone would be put in place," he said. "And then we play out the computer side of that war in the virtual space and challenge our students with what they could expect to see from an adversary in that area."

For example, an adversary might be attempting to gain access to the Air Force's systems or steal intelligence on its operations prior to their launch and possibly send corrupt data to confuse an operation.

Steve said the graduates of his program work with Cyber Command to consider and develop all options, defensive or offensive.

The Washington Post and other news sources have reported the United States and Israel developed the Flame computer virus to slow Iranian nuclear efforts. Israel has also admitted it is involved in offensive cyber warfare operations.

Steve, however, would not give specifics about offensive measures and mostly talked about the defensive systems he teaches.

To protect an F-15, for example, it's necessary to identify all the dependencies the aircraft might have in the cyber world before it goes out on a mission. The preparation for the flight, the course it will take and where it will need to stop to refuel are some areas that could be planned on a computer network.

The key is to be wary of anything that looks suspicious, he said.

"If an F-15 is flying a sortie off of bad data, they could be in the wrong place or they could miss a refueling point," Steve said. "Students learn to identify the abnormal."

Table of Contents

Four Ways the Internet Could Go Down

By David Eagleman, CNN, July 10, 2012

The Internet was designed to be robust, fault-tolerant and distributed, but its technology is still in its infancy.

The fact that the Web has not stopped functioning in its initial decades sometimes encourages us to assume that it never will. But like any system, biological or man-made, the Internet has the potential to fail.

Monday's "DNSChanger" malware problem, which affected some 200,000 computers, was much hyped and ultimately inconsequential. But here are four maladies that really do have the potential to wipe out Internet access on a massive scale.

1. Space weather

When you think about Web surfing, you probably don't worry about what's happening on the surface of the sun 92 million miles away. But you should. Solar flares are one of our most serious threats for our communication systems.

Consider satellite failures. One afternoon in 1998, the Galaxy IV, a $250 million satellite floating 35,000 kilometers above the planet, suddenly spun out of control. The main suspect is a solar flare: the sun was acting up at that time, and several other satellites (owned by Germany, Japan, NASA and Motorola) all failed at the same moment.

The effects were instant and worldwide. Eighty percent of pagers instantly went down. Physicians, managers and drug dealers all across the United States looked down and realized they were no longer receiving pages. NPR, CBS, Direct PC Internet and dozens of other services went down. It is estimated that in recent years at least 12 satellites have been lost due to the effects of space weather.

But it's not just satellites that we have to worry about. When a massive solar flare erupts on the sun, it can cause geomagnetic storms on the Earth. The largest solar eruption recorded so far was in 1859. Known as the Carrington flare, it sent telegraph wires across Europe and America into a sparking frenzy.

Since that time, the technology blanketing the planet has changed quite a bit. If we were to get another solar flare of that size now, what would happen? The answer is clear to space physicists and electrical engineers: it would blow out transformers and melt down our computer systems. In a small disruption in 1989, an electromagnetic storm arrested power throughout most of Quebec and halted the Toronto stock market for three hours.

A major solar event could theoretically melt down the whole Internet. What earthquakes, bombs, and terrorism cannot do might be accomplished in moments by a solar corona.

Given our dependence on the communication systems of our planet, both satellite- and ground-based, this is not simply a theoretical worry. The next major geomagnetic storms are expected at the peak of the next solar sunspot cycle in mid-2013, so hang on tight.

2. Cyberwarfare

Wars of the future will be fought less by rugged soldiers in the field and more by smart kids perched in front of computers slamming energy drinks. As our dependence shifts onto the Net, so do our vulnerabilities.

This future can already be detected in the tight relationship between corporeal conflicts and cyber attacks. When one examines the physical conflicts between India and Pakistan, the Israelis and Palestinians or the parties in the collapse of Yugoslavia, the escalation of real-world violence is immediately mirrored by cyber-space warfare.

The main targets in cyberwar are largely military targets, but increasingly large multinational corporations serve just as well. Take one of them down, even temporarily, and you have done more damage to the economy of your enemy than scores of soldier deaths.

Since the beginning of the computer era, the 1960s, there have been computer viruses: programs that latch onto a host system to reproduce themselves and send out new copies. Just as in biology, as computers have evolved in sophistication, so have viruses co-evolved. And the cousins to the viruses, worms, do not even need a host system but can multiply themselves over networks.

Given the defenses in place, are these parasites only a minor theoretical concern? No. Consider the Stuxnet worm that raised its head in 2010. This worm zigzagged its way into Iranian industrial systems, reprogrammed them, hid its tracks and wrecked the factory operations. Seemingly coming from nowhere, Stuxnet introduced itself as a destructive, unstoppable herald of what's to come.

It will surprise no one that cyberwarfare of the future will involve targeting not only military and industrial targets but Internet connectivity for the general population. If you want to take down your enemy, start by shredding his Net.

3. Political mandate

In the face of the 2010 post-election riots in Iran, the government there shut down the Internet for 45 minutes, presumably to set up filtering of YouTube, Twitter and other sites. Egypt did the same during its revolution of early 2011. China is actively pursuing the capability to shut down its own Internet this way.

But it's not just countries like Iran and China that think about this kind of control over the Web. On June 24, 2010, a Homeland Security committee in the U.S. Senate approved a bill giving the president authority to wield an "Internet kill switch." The bill, Protecting Cyberspace as a National Asset Act (PCNAA), proposed to give the president "emergency authority to shut down private sector or government networks in the event of a cyber attack capable of causing massive damage or loss of life."

The "kill switch" provision was removed from the version of the cybersecurity bill that's before the current Congress.

It's probably just as well. Almost unanimously, Internet security analysts feel that shutting down the Web would inevitably do more harm than good, given our predicted level of dependency on it in time of war for news, communication with loved ones and crisis information aggregation.

Security guru Bruce Schneier identifies at least 3 problems with the shutdown idea. First, the hope of building an electronic line of fortifications is flawed because there will always be hundreds of ways for enemies to get around it. No nation or legal decree can plug all the holes.

The second major problem is that we will be entirely unable to predict the effects of such an attempted shutdown. As Schneier puts it: "The Internet is the most complex machine mankind has ever built and shutting down portions of it would have all sorts of unforeseen ancillary effects."

The third major problem is the security hole it exposes. Once a domestic Internet kill switch has been built, why would a cyberattacker concentrate his efforts on anything else?

Given that the number of people who could use the Internet for good in a crisis situation will presumably outnumber the bad guys, it is probably best to not cut off our heavy dependence on the Web just as things are going bad. Given that a recent survey by Unisys found 61% of Americans approve of the Internet kill-switch concept, this issue will require constant vigilance.

Tell your congressmen: Back away from the switch, slowly.

4. Cable cutting

Although satellites are used for some Internet traffic, more than 99 percent of global Web traffic is dependent on deep-sea networks of fiber-optic cables that blanket the ocean floor like a nervous system. These are a major physical target in wars, especially at special choke-points in the system. And this is not simply a theoretical prediction, the underwater battles are well underway.

As much as three-fourths of the international communications between the Middle East and Europe have been carried by two undersea cables: SeaMeWe-4 and FLAG Telecom's FLAG Europe-Asia cable. On January 30, 2008, both of these cables were cut, severely disrupting Internet and telephone traffic from India to Egypt.

It is still not clear how the cables were cut, or by whom. And for that matter, it is not clear how many cables were cut: some news reports suggest that there were at least eight. Initial speculations proposed that the cuts came from a ship anchor, but a video analysis soon revealed there were no ships in that region from 12 hours before until 12 hours after the slice.

Those cables were only the beginning. A few days later, on February 1, 2008, an undersea FLAG Falcon cable in the Persian Gulf was cut 55 miles off the coast of Dubai. On February 3rd, a cable between the United Arab Emirates and Qatar was cut. On February 4th, the Khaleej Times reported that not only these cables, but also two more, a Persian Gulf cable near Iran, and a SeaMeWe4 cable off the coast of Malaysia.

These cuts led to widespread outages of the Internet, especially in Iran. Suspicions that this reflected underwater sabotage derived in no small part from the geographical pattern: almost all the cables were cut in Middle Eastern waters near Muslim nations. Who might have done it? No one knows. But it is known that the U.S. Navy has deployed undersea special operations for decades. In Operation Ivy Bells, for example, Navy divers appear to have swum from submarines to tap an undersea cable in the Kuril Islands.

Whatever the truth behind the incident, we see that if a government or organization wants badly enough to sabotage the telecommunications across a wide swath, it is possible. New deep-sea cables are urgently needed to protect the global economy because businesses worldwide are vulnerable to the targeting of "choke points" in underwater communications.

Whether by terrorists, governments or cyber-pirates, these weak points in the chain should be keeping us all up at night.

What to do about it

The Global Seed Vault in Svalbard (a small island in the Arctic) is a secure bank for the future of the world. It holds duplicate samples -- that is, spare copies -- of seeds held in gene banks worldwide. The seed vault provides insurance in the event of large-scale regional or global crises.

If a nuclear winter, say, were to wipe out all the crops on the planet, future generations could reboot the agricultural system by hoofing it out to Svalbard.

I propose that we need to have a similar backup security plan for the human knowledge that underlies the Internet.

I'm not suggesting something like the Way Back Machine, which takes snapshots of websites through time. I'm instead talking about simple instructions, burned onto physical media, for how to generate electricity, how to build a computer, how to build a router and how to reconstitute the Internet from basic principles.

The Web appears to be the single most important technology that has ever been invented. We have been the generation lucky enough to witness its inception, and we are now the ones responsible for its protection.

Table of Contents

Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight

From Military & Aerospace Electronics, 10 July 2012

[My note: full report with the tables, figures, and appendices found at GAO website]

GAO-12-479

GAO Report to Committee on Armed Services House of Representatives

Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight

July 9, 2012

The Honorable Howard P. ``Buck`` McKeon Chairman The Honorable Adam Smith Ranking Member Committee on Armed Services House of Representatives

The Department of Defense (DOD) is increasingly dependent on access to the electromagnetic spectrum--the full range of all possible frequencies of electromagnetic radiation, including frequency ranges such as radio, microwave, infrared, visible, ultraviolet, X-rays, and gamma rays--for a variety of military uses, such as communicating, navigating, information gathering and sensing, and targeting. DOD has committed billions of dollars developing, maintaining, and employing warfighting capabilities that rely on access to the electromagnetic spectrum--including precision-guided munitions and command, control, and communications systems. DOD ensures control of the electromagnetic spectrum through the coordinated implementation of joint electromagnetic spectrum operations, which includes electronic warfare and spectrum management activities, with other lethal and nonlethal operations that enable freedom of action in the electromagnetic operational environment. Electronic warfare, which is the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack the enemy, is essential for protection of friendly operations and denying adversary operations within the electromagnetic spectrum throughout the operational environment. As we previously reported, DOD`s investments are projected to total more than $17.6 billion from fiscal years 2007 through 2016 for the development and procurement of new and updated fixed-wing airborne electronic attack systems alone, which are one element of electronic warfare.[Footnote 1]

According to DOD, the U.S. military`s access to and use of the electromagnetic spectrum is facing rapidly evolving challenges and increased vulnerabilities due to the increasing quality and availability of electronic warfare capabilities to both state and non- state actors. Also, DOD has reported that electronic warfare capabilities, which play a critical and potentially growing role as an enabler for military operations, are currently stressed and will remain so in the future. Moreover, according to DOD, near- peer competitors, primarily Russia and China, have fully recognized the critical nature of electromagnetic spectrum control in military operations.[Footnote 2] There also has been recognition among near- peer competitors of the relationship between electronic warfare and cyberspace operations, which includes computer network operations. [Footnote 3] For example, as noted in the U.S.-China Economic and Security Review Commission`s 2009 report to Congress, China`s Integrated Network Electronic Warfare department incorporates elements of cyberspace operations in tandem with elements of traditional electronic warfare, and advocates for the employment of traditional electronic warfare operations -such as the jamming of radars and communications systems -in coordination with cyberspace attack operations.

DOD has identified persistent electronic warfare capability gaps, and these shortfalls have been consistently highlighted by the combatant commands as some of their highest war fighting priorities. According to a Center for Strategic and International Studies report, the U.S. Strategic Command identified 34 capability gaps affecting electronic warfare, including a lack of leadership across the department. [Footnote 4] This lack of leadership was identified as the most critical gap. In our recent report on DOD`s airborne electronic attack capabilities, we found that DOD is developing multiple systems which provide similar capabilities, and that the lack of leadership may undermine DOD`s ability to consolidate these systems.[Footnote 5] Specifically, we found that all four military services within the Department of Defense are separately acquiring new airborne electronic attack systems, but that opportunities may exist to consolidate some current service-specific acquisition efforts. With the prospect of slowly growing or flat defense budgets for years to come, the department must get better returns on its weapon system investments and find ways to deliver more capability to the warfighter for less than it has in the past. Therefore, we recommended that the Secretary of Defense conduct program reviews for certain new, key systems; determine the extent to which the most pressing capability gaps can be met and take steps to fill them; align service investments in science and technology with the departmentwide electronic warfare priority; and review the capabilities provided by certain existing and planned systems to ensure investments do not overlap. DOD generally concurred with our recommendations.

You requested that we examine several issues related to DOD`s electronic warfare capabilities. In March 2012, we issued a report on DOD`s current and planned airborne electronic attack capabilities and investment strategies.[Footnote 6] In this current review, we examined DOD`s approach to governing electronic warfare and the relationship between electronic warfare and cyberspace operations. Specifically, we examined the extent to which DOD has (1) developed a strategy to manage electronic warfare and (2) planned, organized, and implemented an effective governance structure to oversee its electronic warfare policy and programs, and their relationship to cyberspace operations.

To assess the extent to which DOD has developed a strategy to manage electronic warfare, we compared information found in DOD`s two electronic warfare strategy reports to Congress with key characteristics of strategies identified by GAO in prior work, and interviewed relevant officials. To assess the extent to which DOD has planned, organized, and implemented an effective governance structure to oversee its electronic warfare policy and programs and their relationship to cyberspace operations, we reviewed DOD directives and policies, and the roles and responsibilities of the Under Secretary of Defense for Policy; Under Secretary of Defense for Acquisition, Technology, and Logistics; and U.S. Strategic Command. Additionally, we reviewed and analyzed information found in policy documents along with information from relevant meetings with DOD officials against DOD`s directives regarding electronic warfare. We also interviewed cognizant officials and reviewed DOD policies, doctrine, reports, plans, and concepts of operation, and outside studies that discuss the relationship between electronic warfare and cyberspace operations. See Appendix I for details on our scope and methodology.

We conducted this performance audit from July 2011 to July 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Control and Use of the Electromagnetic Spectrum

In modern warfare, military forces are heavily dependent upon access to the electromagnetic spectrum for successful operations. Communications with friendly forces and detection, identification, and targeting of enemy forces, among other tasks, are all reliant upon the ability to operate unhindered in the spectrum. For this reason, control of the electromagnetic spectrum is considered essential to carrying out military operations.[Footnote 7] Figure 1 illustrates the electromagnetic spectrum and some examples of military uses at various frequencies. For example, infrared or thermal imaging technology senses heat emitted by a person or an object and creates an image. Sensor systems utilize this technology to provide the advantage of seeing not only at night but also through smoke, fog, and other obscured battlefield conditions.

Electronic Warfare

DOD defines electronic warfare as any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The purpose of electronic warfare is to secure and maintain the freedom of action in the electromagnetic spectrum for friendly forces and to deny the same for the adversary. Traditionally, electronic warfare has been composed of three primary activities

-- Electronic attack use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Electronic attack can be used offensively, such as jamming enemy communications or jamming enemy radar to suppress its air defenses, and defensively, such as deploying flares.

-- Electronic protection actions to protect personnel, facilities, and equipment from any effects of friendly, neutral, or enemy use of the electromagnetic spectrum, as well as naturally occurring phenomena that degrade, neutralize, or destroy friendly combat capability.

-- Electronic warfare support actions directed by an operational commander to search for, intercept, identify, and locate sources of radiated electromagnetic energy for the purposes of immediate threat recognition, targeting, and planning; and conduct of future operations.

Information Operations

Electronic warfare is employed to create decisive stand-alone effects or to support military operations, such as information operations and cyberspace operations. According to DOD, information operations are the integrated employment, during military operations, of information- related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Information- related capabilities can include, among others, electronic warfare, computer network operations, military deception, operations security, and military information support operations (formerly psychological operations). Electronic warfare contributes to the success of information operations by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the electromagnetic spectrum while protecting U.S. and allied freedom of action.

Cyberspace Operations

Since cyberspace requires both wired and wireless links to transport information, both offensive and defensive cyberspace operations may require use of the electromagnetic spectrum. According to DOD, cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve military objectives or effects through cyberspace, which include computer network operations, among others. Computer network operations include computer network attack, computer network defense, and related computer network exploitation- enabling operations. Electronic warfare and cyberspace operations are complementary and have potentially synergistic effects. For example, an electronic warfare platform may be used to enable or deter access to a computer network.

U.S. Strategic Command Joint Electronic Warfare Activities

U.S. Strategic Command (Strategic Command) has been designated since 2008 as the advocate for joint electronic warfare. Strategic Command officials stated that, in the past, the primary office for electronic warfare expertise--the Joint Electronic Warfare Center--had several different names and was aligned under several different organizations, such as the Joint Forces Command and the U.S. Space Command.

According to Strategic Command officials, in addition to the Joint Electronic Warfare Center, the command employs electronic warfare experts in its non-kinetic operations staff and in the Joint Electromagnetic Preparedness for Advanced Combat organization. According to Strategic Command officials, the Joint Electronic Warfare Center is the largest of the three organizations and employs approximately 60 military and civilian electronic warfare personnel and between 15 and 20 contractors. Strategic Command officials stated that the Joint Electronic Warfare Center was created as a DOD center of excellence for electronic warfare and has electronic warfare subject matter experts. The center provides planning and technical support not only to Strategic Command but to other combatant commands and organizations, such as U.S. Central Command, U.S. European Command, U.S. Pacific Command, and the Department of Homeland Security. The Joint Electronic Warfare Center also provides assistance with requirements generation to the military services.

DOD Developed an Electronic Warfare Strategy, but Only Partially Addressed Key Desirable Strategy Characteristics

DOD developed an electronic warfare strategy, but only partially addressed key strategy characteristics identified as desirable in prior work by GAO. The National Defense Authorization Act for Fiscal Year 2010 requires the Secretary of Defense to submit to the congressional defense committees an annual report on DOD`s electronic warfare strategy for each of fiscal years 2011 through 2015.[Footnote 8] Each annual report is to be submitted at the same time the President submits the budget to Congress and is to contain, among other things, a description and overview of DOD`s electronic warfare strategy and the organizational structure assigned to oversee the development of the department`s electronic warfare strategy, requirements, capabilities, programs, and projects.[Footnote 9] In response to this legislative requirement, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics issued DOD`s 2011 and 2012 fiscal year strategy reports to Congress in October 2010 and November 2011, respectively.[Footnote 10]

We previously reported that it is desirable for strategies to delineate six key characteristics, including organizational roles and responsibilities for implementing parties as well as performance measures to gauge results.[Footnote 11] The key characteristics of an effective strategy can aid responsible parties in further developing and implementing the strategy, enhance the strategy`s usefulness in resource and policy decisions, and better ensure accountability. The six characteristics are (1) purpose, scope, and methodology; (2) problem definition and risk assessment; (3) goals, subordinate objectives, activities, and performance measures; (4) resources, investments, and risk management; (5) organizational roles, responsibilities, and coordination; and (6) integration and implementation.

As illustrated in Figure 3, we found that DOD`s reports addressed two key characteristics, but only partially addressed four other key characteristics of a strategy. For example, the strategy reports to Congress included elements of characteristics, such as a goal and objectives, but did not fully identify implementing parties, delineate roles and responsibilities for managing electronic warfare across the department, or identify outcome- related performance measures that could guide the implementation of electronic warfare efforts and help ensure accountability. Similarly, the reports provided acquisition program and research and development project data, but did not target resources and investments at some key activities associated with implementing the strategy. When investments are not tied to strategic goals and priorities, resources may not be used effectively and efficiently. Our past work has shown that such characteristics can help shape policies, programs, priorities, resource allocations, and standards in a manner that is conducive to achieving intended results. [Footnote 12]

DOD`s fiscal year 2011 report is described here because the fiscal year 2012 report, issued in November 2011, is classified. However, unclassified portions of this document note that the fiscal year 2011 report remains valid as the base DOD strategy and that the fiscal year 2012 report updates its predecessor primarily to identify ongoing efforts to improve DOD`s electronic warfare capabilities and to provide greater specificity to current threats. The fiscal year 2011 Electronic Warfare Strategy of the Department of Defense report (electronic warfare strategy report)--the base electronic warfare strategy--addressed two and partially addressed four of six desirable characteristics of a strategy identified by GAO. There may be considerable variation in the extent to which the strategy addressed specific elements of those characteristics that were determined by GAO to be partially addressed. Our analysis of the fiscal year 2011 report`s characteristics is as follows.

-- Purpose, scope and methodology Addressed. The fiscal year 2011 electronic warfare strategy report identifies the purpose of the strategy, citing as its impetus section 1053 of the National Defense Authorization Act for Fiscal Year 2010, and articulates a maturing, twofold strategy focused on integrating electronic warfare capabilities into all phases and at all levels of military operations, as well as developing, maintaining, and protecting the maneuver space within the electromagnetic spectrum necessary to enable military capabilities. The report`s scope also encompasses data on acquisition programs and research and development projects. Additionally, the report includes some methodological information by citing a principle that guided its development. Specifically the report states that a key aspect of the strategy is the concept of the electromagnetic spectrum as maneuver space.

-- Problem definition and risk assessment Addressed. The fiscal year 2011 electronic warfare strategy report defines the problem the strategy intends to address, citing the challenges posed to U.S. forces by potential adversaries` increasingly sophisticated technologies, the military`s increased dependence on the electromagnetic spectrum, and the urgent need to retain and expand remaining U.S. advantages. The report also assesses risk by identifying threats to, and vulnerabilities of critical operations, such as Airborne Electronic Attack and self- protection countermeasures.

-- Goals, subordinate objectives, activities, and performance measures Partially Addressed. The fiscal year 2011 electronic warfare strategy report communicates an overarching goal of enabling electromagnetic spectrum maneuverability and cites specific objectives, such as selectively denying an adversary`s use of the spectrum and preserving U.S. and allied forces` ability to maneuver within the spectrum. The report also identifies key activities associated with the strategy, including developing (1) coherent electronic warfare organizational structures and leadership, (2) an enduring and sustainable approach to continuing education, and (3) capabilities to implement into electronic warfare systems. The report does not identify performance measures that could be used to gauge results and help ensure accountability.

-- Resources, investments, and risk management Partially Addressed. The fiscal year 2011 electronic warfare strategy report broadly targets resources and investments by emphasizing the importance of continued investment in electronic attack, electronic protection, and electronic support capabilities. The report also notes some of the associated risks in these areas, calling for new methods of ensuring U.S. control over the electromagnetic spectrum in light of the adversary`s advances in weapons and the decreasing effectiveness of traditional lines of defense, such as airborne electronic attack and self-protection countermeasures. The report identifies some of the costs associated with the strategy by providing acquisition program and research and development project and cost data, and notes that part of the strategy is to identify and track investments in electronic warfare systems, which often are obscured within the development of the larger weapons platforms they typically support. However, the strategy does not target investments by balancing risk against costs, or discuss other costs associated with implementing the strategy by, for example, targeting resources and investments at key activities, such as developing electronic warfare organizational structures and leadership and developing an enduring and sustainable approach to continuing education.

-- Organizational roles, responsibilities, and coordination Partially Addressed. The fiscal year 2011 electronic warfare strategy report provides an overview of past and ongoing electronic warfare activities within the military services and DOD, and identifies several mechanisms that have or could be used to foster coordination across the department. For example, it outlines the Army`s efforts to create a new career field for electronic warfare officers and the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics` electronic warfare integrated planning team.[Footnote 13] However, the report does not fully identify the departmental entities responsible for implementing the strategy, discuss the roles and responsibilities of implementing parties, or specify implementing entities` relationships in terms of leading, supporting, and partnering.[Footnote 14]

-- Integration and implementation Partially Addressed. The fiscal year 2011 electronic warfare strategy report describes the department`s approach to ensuring maneuverability within the electromagnetic spectrum, thus supporting National Defense Strategy objectives that rely on use and control of the spectrum. The strategy`s overarching aim of ensuring electromagnetic spectrum maneuverability also is consistent with concepts contained in the department`s electromagnetic spectrum strategy documents--which collectively emphasize the importance of assured spectrum access.[Footnote 15] The strategy does not, however, discuss the department`s plans for implementing the strategy.

DOD`s electronic warfare strategy reports were issued in response to the National Defense Authorization Act for Fiscal Year 2010 and were not specifically required to address all the characteristics we consider to be desirable for an effective strategy. Additionally, DOD`s fiscal year 2011 report states that the strategy is still maturing and that subsequent reports to Congress will refine the department`s vision. Nonetheless, we consider it useful for DOD`s electronic warfare strategy to address each of the characteristics we have identified in order to provide guidance to the entities responsible for implementing DOD`s strategy and to enhance the strategy`s utility in resource and policy decisions--particularly in light of the diffuse nature of DOD`s electronic warfare programs and activities, as well as the range of emerging technical, conceptual, and organizational challenges and changes in this area. Further, in the absence of clearly defined roles and responsibilities, and other elements of key characteristics, such as measures of performance in meeting goals and objectives, entities responsible for implementing DOD`s strategy may lack the guidance necessary to establish priorities and milestones, thereby impeding their ability to achieve intended results within a reasonable time frame. As a result, DOD lacks assurance that its electronic warfare programs and activities are aligned with strategic priorities and are managed effectively. For example, without an effective strategy, DOD is limited in its ability to reduce the potential for unnecessary overlap in the airborne electronic attack acquisition activities on which we have previously reported.

DOD Has Not Established an Effective Departmentwide Governance Framework for Managing and Overseeing Electronic Warfare

DOD has taken some steps to address a critical leadership gap identified in 2009, but it has not established a departmentwide governance framework for planning, directing, and controlling electronic warfare activities. DOD is establishing a Joint Electromagnetic Spectrum Control Center (JEMSCC) under Strategic Command in response to the leadership gap for electronic warfare. However, DOD has not documented the objectives or implementation tasks and timeline for the JEMSCC. In addition, DOD has not updated key guidance to reflect recent policy changes regarding electronic warfare management and oversight roles and responsibilities. For example, it is unclear what the JEMSCC`s role is in relation to other DOD organizations involved in the management of electronic warfare, such as the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Moreover, we found that DOD may face challenges in its oversight of electronic warfare as a result of the evolving relationship between electronic warfare and cyberspace operations.

DOD Actions Have Not Fully Addressed a Critical Leadership Gap

DOD has taken some steps to address a critical leadership gap by establishing the JEMSCC under Strategic Command. However, because DOD has yet to define specific objectives for the center, outline major implementation tasks, and define metrics and timelines to measure progress, it is unclear to what extent the center will address the identified existing leadership deficiencies. The Center for Strategic and International Studies reported insufficient leadership as the most critical among 34 capability gaps affecting electronic warfare. As a result of the absence of leadership, the department was significantly impeded from both identifying departmentwide needs and solutions and eliminating potentially unnecessary overlap among the military services` electronic warfare acquisitions. Specifically, the department lacked a joint leader and advocate with the authority to integrate and influence electronic warfare capabilities development, to coordinate internal activities, and to represent those activities and interests to outside organizations. Mitigating the leadership gap was identified not only as the highest priority, but also a prerequisite to addressing the other 33 gaps.

The Center for Strategic and International Studies report was one of two parallel studies commissioned by the Joint Requirements Oversight Council[Footnote 16] to assess potential organizational and management solutions to the leadership gap.[Footnote 17] These studies considered a number of options, including an organization under the Deputy Secretary of Defense, an activity controlled by the Chairman of the Joint Chiefs of Staff, and an organization at Strategic Command. As a result of these studies, in January 2011, DOD initiated efforts to establish the JEMSCC under Strategic Command as the focal point of joint electronic warfare advocacy. This solution was chosen, in part, in recognition of Strategic Command`s resident electronic warfare expertise as well as its already assigned role as an electronic warfare advocate.[Footnote 18]

In January 2011, the Joint Requirements Oversight Council directed Strategic Command to develop an implementation plan for the electronic warfare center to be submitted for council approval no later than May 2011. The plan was to delineate (1) the center`s mission, roles, and responsibilities; (2) command and control, reporting, and support relationships with combatant commands, military services, and U.S. Government departments and agencies; and (3) minimum requirements to achieve initial operational capability and full operational capability. The Joint Requirements Oversight Council subsequently approved an extension of the center`s implementation plan submission to August 2011. Subsequently, in December 2011, the oversight council issued a memorandum that closed the requirement to submit an implementation plan to the council and stated that Strategic Command had conducted an internal reorganization and developed a center to perform the functions identified in the internal DOD study.

In December 2011, Strategic Command issued an operations order that defined the JEMSCC as the primary focal point for electronic warfare, supporting DOD advocacy for joint electronic warfare capability requirements, resources, strategy, doctrine, planning, training, and operational support. This order provided 22 activities that the center is to perform. Federal internal control standards require that organizations establish objectives and clearly define key areas of authority and responsibility.[Footnote 19] In addition, best practices for strategic planning have shown that effective and efficient operations require detailed plans outlining major implementation tasks and defined metrics and timelines to measure progress.[Footnote 20] Moreover, the independent study prepared for DOD similarly emphasized the importance of clearly defining the center`s authorities and responsibilities, noting that the center`s success would hinge, in part, on specifying how it is expected to relate to the department as a whole as well as its expected organizational outcomes. However, as of March 2012, Strategic Command had not issued an implementation plan or other documentation that defines the center`s objectives and outlines major implementation tasks, metrics, and timelines to measure progress. Strategic Command officials told us in February 2012 that an implementation plan had been drafted, but that there were no timelines for the completion of the implementation plan or a projection for when the center would reach its full operational capability. As a result, it remains unclear whether or when the JEMSCC will provide effective departmentwide leadership and advocacy for electronic warfare, and influence resource decisions related to capability development.

According to officials from Strategic Command, the JEMSCC will consist of staff from Strategic Command`s Joint Electronic Warfare Center at Lackland Air Force Base, Texas, and the Joint Electromagnetic Preparedness for Advanced Combat organization, at Nellis Air Force Base, Nevada.[Footnote 21] These officials stated that while each of JEMSCC`s component groups` missions will likely evolve as the center matures, the JEMSCC components would continue prior support activities, such as the Joint Electronic Warfare Center`s support to other combatant commands through its Electronic Warfare Planning and Coordination Cell--a rapid deployment team that provides electronic warfare expertise and support to build electronic warfare capacity. Figure 4 depicts the JEMSCC`s organizational construct.

DOD has yet to define objectives and issue an implementation plan for the JEMSCC; however, officials from Strategic Command stated that they anticipated continuity between the command`s previous role as an electronic warfare advocate and its new leadership role, noting that advocacy was, and remains, necessary because electronic warfare capabilities are sometimes undervalued in comparison to other, kinetic capabilities.[Footnote 22] For example, the JEMSCC will likely build off Strategic Command`s previously assigned advocacy role, in part, by continuing to advocate for electronic warfare via the Joint Capabilities Integration and Development System process--DOD`s process for identifying and developing capabilities needed by combatant commanders--and by providing electronic warfare expertise.[Footnote 23] Specifically, Strategic Command officials stated that the JEMSCC, through Strategic Command, would likely provide input to the development of joint electronic warfare requirements during the joint capabilities development process. However, combatant commands, such as Strategic Command, provide one of many inputs to this process. Further, as we have previously reported, council decisions, while influential, are advisory to acquisition and budget processes driven by military service investment priorities.[Footnote 24] As a result, the JEMSCC`s ability to affect resource decisions via this process is likely to be limited.

Officials we spoke with across DOD, including those from the military services and Strategic Command, recognized this challenge. Specifically, Strategic Command officials told us that for JEMSCC to influence service-level resource decisions and advocate effectively for joint electronic warfare capabilities, the JEMSCC would need to not only participate in the joint capabilities development process, but would also need authorities beyond those provided by the Unified Command Plan, such as the authority to negotiate with the military services regarding resource decisions. Similarly, we found that while the officials we spoke with from several DOD offices that manage electronic warfare, including offices within the military services, were unaware of the center`s operational status and unclear regarding its mission, roles, and responsibilities, many also thought it to be unlikely that the JEMSCC--as a subordinate center of Strategic Command--would possess the requisite authority to advocate effectively for electronic warfare resource decisions. These concerns were echoed by the independent study, which noted that the center would require strong authorities to substantially influence the allocation of other DOD elements` resources.[Footnote 25]

Additionally, limited visibility across the department`s electronic warfare programs and activities may impede the center`s ability to advocate for electronic warfare capabilities development. Specifically, Strategic Command officials told us that they do not have access to information regarding all of the military services` electronic warfare programs and activities, particularly those that are highly classified or otherwise have special access. In addition, Strategic Command officials told us that they do not have visibility over or participate in rapid acquisitions conducted through the joint capabilities development process. In our March 2012 report on DOD`s airborne electronic attack strategy and acquisitions, we reported that certain airborne electronic attack systems in development may offer capabilities that unnecessarily overlap with one another--a condition that appears most prevalent with irregular warfare systems that the services are acquiring under DOD`s rapid acquisitions process. [Footnote 26] The JEMSCC`s exclusion from this process is likely to limit its ability to develop the departmentwide perspective necessary for effective advocacy. Moreover, in the absence of clearly defined objectives and an implementation plan outlining major implementation tasks and timelines to measure progress, these potential challenges reduce DOD`s level of assurance that the JEMSCC will provide effective departmentwide leadership for electronic warfare capabilities development.

DOD Policy Documents Have Not Been Updated to Include All Oversight Roles and Responsibilities for Electronic Warfare

DOD issued two primary directives that provide some guidance for departmentwide oversight of electronic warfare. However, neither of these two directives has been updated to reflect changes in DOD`s leadership structures that manage electronic warfare. Federal internal control standards require that organizations establish objectives, clearly define key areas of authority and responsibility, and establish appropriate lines of reporting to aid in the effective and efficient use of resources.[Footnote 27] Additionally, those standards state that management must continually assess and evaluate its internal control to assure that the actions in place are effective and updated when necessary.

DOD`s two primary directives that provide some guidance for departmentwide oversight of electronic warfare are

-- DOD Directive 3222.4 (Electronic Warfare and Command and Control Warfare Countermeasures)--Designates the Under Secretary of Defense for Acquisition (now Acquisition, Technology, and Logistics) as the focal point for electronic warfare within the department. However, the directive was issued in 1992 and updated in 1994, and does not reflect subsequent changes in policy or organizational structures. For example, the directive does not reflect the establishment of the JEMSCC under Strategic Command.

-- DOD Directive 3600.01 (Information Operations)--Issued in 2006 and revised in May 2011, this directive provides the department with a framework for oversight of information operations, which was defined as the integrated employment of the core capabilities of electronic warfare, computer network operations, military information support operations (formerly referred to as psychological operations), military deception, and operations to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting that of the United States. However, the definition of oversight responsibilities for information operations has changed, and these changes have not yet been reflected in DOD Directive 3600.01.[Footnote 28]

DOD Directive 3222.4 has not been updated to reflect the responsibilities for electronic warfare assigned to Strategic Command. Both the December 2008 and April 2011 versions of the Unified Command Plan assigned Strategic Command responsibility for advocating for joint electronic warfare capabilities.[Footnote 29] Similarly, the directive has not been updated to reflect the establishment of the JEMSCC and its associated electronic warfare responsibilities. Specifically, the directive does not acknowledge that JEMSCC has been tasked by Strategic Command as the primary focal point for electronic warfare; rather, the directive designates the Under Secretary of Defense for Acquisition, Technology, and Logistics as the focal point for electronic warfare within DOD. As a result, it is unclear what JEMSCC`s roles and responsibilities are in relation to those of the Under Secretary of Defense for Acquisition, Technology, and Logistics. For example, it`s unclear what JEMSCC`s role will be regarding development of future iterations of the DOD`s electronic warfare strategy report to Congress, which is currently produced by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Also it is unclear what role, if any, the JEMSCC will have in prioritizing electronic warfare investments. Moreover, the directive has not been updated to reflect the Secretary of Defense`s memorandum issued in January 2011, which assigned individual capability responsibility for electronic warfare and computer network operations to Strategic Command.

DOD Directive 3600.01 provides both the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Under Secretary of Defense for Intelligence with responsibilities that aid in the oversight of electronic warfare within DOD. However, pursuant to the Defense Secretary`s January 2011 memo, the directive is under revision to accommodate changes in roles and responsibilities. Under the current version of DOD Directive 3600.01, the Under Secretary of Defense for Intelligence is charged with the role of Principal Staff Advisor to the Secretary of Defense for information operations. The Principal Staff Advisor is responsible for, among other things, the development and oversight of information operations policy and integration activities as well as the coordination, oversight, and assessment of the efforts of DOD components to plan, program, develop, and execute capabilities in support of information operations requirements.[Footnote 30] Additionally, the current Directive 3600.01 identifies the Under Secretary of Defense for Acquisition, Technology, and Logistics as responsible for establishing specific policies for the development of electronic warfare as a core capability of information operations.

Under the requirements of DOD acquisition policy, the Under Secretary of Defense for Acquisition, Technology, and Logistics regularly collects cost, schedule, and performance data for major programs. [Footnote 31] In some cases, the cost information of electronic warfare systems are reported as distinct programs, while in other cases, some electronic warfare systems are subcomponents of larger programs, and cost information is not regularly collected for these separate subsystems. Additionally, the Under Secretary--in coordination with the Army, the Navy, and the Air Force--is developing an implementation road map for electronic warfare science and technology. The road map is supposed to coordinate investments across DOD to accelerate the development and delivery of capabilities. The road map is expected to be completed in late summer of 2012.

The Secretary of Defense issued a memorandum in January 2011 that prompted DOD officials to begin revising DOD Directive 3600.01. The memorandum redefined information operations as ``the integrated employment, during military operations, of information- related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.`` Previously, DOD defined information operations as the ``integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.`` According to DOD officials, the revised definition removed the term core capabilities because it put too much emphasis on the individual core capabilities and too little emphasis on the integration of these capabilities.

Additionally, the memorandum noted that the Under Secretary of Defense for Policy began serving as the Principal Staff Advisor for information operations as of October 1, 2010, and charged the Under Secretary of

Defense for Policy with revising DOD Directive 3600.01 to reflect these responsibilities. According to the memorandum, the Principal Staff Advisor is to serve as the single point of fiscal and program accountability for information operations. However, according to DOD officials, this accountability oversight covers only the integration of information operations-related capabilities and does not cover the formerly defined core capabilities of information operations, including electronic warfare and computer network operations. For example, DOD officials stated that the Principal Staff Advisor for information operations would maintain program accountability where information operations-related capabilities were integrated but would not maintain program accountability for all information- related capabilities. However, the memorandum does not clearly describe the specific responsibilities of the Principal Staff Advisor for information operations.

The Secretary`s memorandum directed the Under Secretary of Defense for Policy, together with the Undersecretary of Defense (Comptroller) and Director of Cost Analysis and Program Evaluation, to continue to work to develop standardized budget methodologies for information operations-related capabilities and activities. However, these budget methodologies would capture only data related to information operations. For example, according to Under Secretary of Defense for Policy officials, they do not collect or review electronic warfare financial data, but may review this data in the future to determine if it relates to integrated information operations efforts. Officials from the Office of the Under Secretary of Defense for Policy stated that DOD Directive 3600.01 was under revision to reflect these and other changes as directed by the Secretary`s memorandum. Until the underlying directive is revised, there may be uncertainty regarding which office has the authority to manage and oversee which programs. Moreover, until this directive is updated, it is not clear where the boundaries are for oversight of electronic warfare between the Under Secretary of Defense for Policy and the Under Secretary of Defense for Acquisition, Technology, and Logistics.

Table 1 compares the oversight roles and responsibilities for electronic warfare as described in the two DOD directives and the Secretary`s 2011 policy memorandum.

DOD May Face Challenges in Its Oversight of the Evolving Relationship of Electronic Warfare and Cyberspace Operations

DOD may face challenges in its oversight of electronic warfare because of the evolving relationship between electronic warfare and cyberspace operations, specifically computer network operations; both are information operations-related capabilities. According to DOD, to ensure all aspects of electronic warfare can be developed and integrated to achieve electromagnetic spectrum control, electronic warfare must be clearly and distinctly defined in its relationship to information operations (to include computer network operations) and the emerging domain of cyberspace. In the previous section, we noted that DOD`s directives do not clearly define the roles and responsibilities for the oversight of electronic warfare in relation to the roles and responsibilities for information operations. The current DOD Directive 3600.01 does not clearly specify what responsibilities the Principal Staff Advisor has regarding the integration of information operations-related capabilities--specifically the integration of electronic warfare capabilities with computer network operations.[Footnote 32]

Further, DOD`s fiscal year 2011 electronic warfare strategy report to Congress, which delineated its electronic warfare strategy, stated that the strategy has two, often co-dependent capabilities traditional electronic warfare and computer network attack, which is part of cyberspace operations. Moreover, according to DOD officials, the relationship between electronic warfare and cyberspace operations-- including computer network attack--is still evolving, which is creating both new opportunities and challenges. There will be operations and capabilities that blur the lines between cyberspace operations and electronic warfare because of the continued expansion of wireless networking and the integration of computers and radio frequency communications. According to cognizant DOD officials, electronic warfare capabilities may permit use of the electromagnetic spectrum as a maneuver space for cyberspace operations. For example, electronic warfare capabilities may serve as a means of accessing otherwise inaccessible networks to conduct cyberspace operations; presenting new opportunities for offensive action as well as the need for defensive preparations.

Current DOD doctrine partially describes the relationship between electronic warfare and cyberspace operations. Specifically, current joint doctrine for electronic warfare, which was last updated in February 2012, states that since cyberspace requires both wired and wireless links to transport information, both offensive and defensive cyberspace operations may require use of the electromagnetic spectrum for the enabling of effects in cyberspace. Due to the complementary nature and potential synergistic effects of electronic warfare and computer network operations, they must be coordinated to ensure they are applied to maximize effectiveness.[Footnote 33] When wired access to a computer system is limited, electromagnetic access may be able to successfully penetrate the computer system. For example, use of an airborne weapons system to deliver malicious code into cyberspace via a wireless connection would be characterized as ``electronic warfare- delivered computer network attack.`` In addition, the doctrine mentions that electronic warfare applications in support of homeland defense are critical to deter, detect, prevent, and defeat external threats such as cyberspace threats.

DOD has not yet published specific joint doctrine for cyberspace operations, as we previously reported.[Footnote 34] We recommended, among other things, that DOD establish a time frame for deciding whether to proceed with a dedicated joint doctrine publication on cyberspace operations and update existing cyber- related joint doctrine.[Footnote 35] DOD agreed and has drafted, but not yet issued, the joint doctrine for cyberspace operations. According to U.S. Cyber Command officials, it is unclear when the doctrine for cyberspace operations will be issued.

The military services also have recognized the evolving relationship between electronic warfare and cyberspace operations. For example, to address future challenges, the U.S. Army Training and Doctrine Command conducted an assessment on how the Army`s future force will leverage cyberspace operations and found that the Army`s current vocabulary-- including terms such as computer network operations, electronic warfare, and information operations--will become increasingly inadequate. According to the Army, these terms are becoming outdated as the operational environment rapidly changes due to factors such as technologic convergence of computer and telecommunication networks, astonishing rates of technologic advancements, and the global proliferation of information and communications technology. According to a Navy official, the Navy recognizes the evolving relationship between electronic warfare and cyberspace operations and is moving toward defining that relationship. However, the Navy first is working to define the relationship between electronic warfare and electromagnetic spectrum operations. In addition, Air Force Instruction 10-706, Electronic Warfare Operations,[Footnote 36] states that traditional electronic warfare capabilities are beginning to overlap with cyberspace areas, which is resulting in an increased number of emerging targets such as non-military leadership networks and positioning, navigation, and timing networks.

According to U.S. Cyber Command officials, it is important to understand how electronic warfare and cyberspace operations capabilities might be used in an operational setting. Such information could then inform the further development of doctrine. U.S. Cyber Command officials stated that they have participated in regular meetings with representatives from the military services, the National Security Agency, defense research laboratories, and others, to discuss the relationship of electronic warfare and cyberspace operations. Moreover, the Under Secretary for Acquisition, Technology, and Logistics, has established steering committees that are developing road maps for the Secretary of Defense`s seven designated science and technology priority areas--one of which is cyberspace operations and another is electronic warfare.

Conclusions

DOD faces significant challenges in operating in an increasingly complex electromagnetic environment. Therefore, it is important that DOD develop a comprehensive strategy to ensure departmental components are able to integrate electronic warfare capabilities into all phases of military operations and maintain electromagnetic spectrum access and maneuverability. DOD would benefit from a strategy that includes implementing parties, roles, responsibilities, and performance measures, which can help ensure that entities are effectively supporting such objectives, and linking resources and investments to key activities necessary to meet strategic goals and priorities. In the absence of a strategy that fully addresses these and other key elements, the DOD components and military services responsible for implementing this strategy, evaluating progress, and ensuring accountability may lack the guidance necessary to prioritize their activities and establish milestones that are necessary to achieve intended results within a reasonable time frame. Moreover, as a result, DOD may not be effectively managing its electronic warfare programs and activities or using its resources efficiently. For example, an effective strategy could help DOD reduce the potential for unnecessary overlap in the airborne electronic attack acquisition activities on which we have previously reported.

The military`s increasing reliance on the electromagnetic spectrum-- coupled with a fiscally constrained environment and critical gaps in electronic warfare management--highlights the need for an effective governance framework for managing and conducting oversight of the department`s electronic warfare activities. The absence of such a framework can exacerbate management challenges, including those related to developing and implementing an effective strategy and coordinating activities among stakeholders. Without additional steps to define the purpose and activities of the JEMSCC, DOD lacks reasonable assurance that this center will provide effective departmentwide leadership for electronic warfare capabilities development and ensure the effective and efficient use of its resources. As we previously reported, DOD acknowledges a leadership void that makes it difficult to ascertain whether the current level of investment is optimally matched with the existing capability gaps. Leveraging resources and acquisition efforts across DOD-- not just by sharing information, but through shared partnerships and investments-- can simplify developmental efforts, improve interoperability among systems and combat forces, and could decrease future operating and support costs. Such successful outcomes can position the department to maximize the returns it gets on its electronic warfare investments. In addition, multiple organizations are involved with electronic warfare and outdated guidance regarding management and oversight may limit the effectiveness of their activities. Both the Under Secretary of Defense for Acquisition, Technology, and Logistics and the JEMSCC have been identified as the focal point for electronic warfare within the department, yet it is unclear what each organization`s roles and responsibilities are in relation to one another. Further, each organization`s management responsibilities related to future iterations of the electronic warfare strategy report to Congress and working with the military services to prioritize investments remain unclear. Updating electronic warfare directives and policy documents to clearly define oversight roles and responsibilities for electronic warfare--including any roles and responsibilities related to managing the relationship between electronic warfare and information operations or electronic warfare and cyberspace operations, specifically computer network operations--would help ensure that all aspects of electronic warfare can be developed and integrated to achieve electromagnetic spectrum control.

Recommendations for Executive Action

To improve DOD`s management, oversight, and coordination of electronic warfare policy and programs, we recommend that the Secretary of Defense take the following three actions

-- Direct the Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the Under Secretary of Defense for Policy and Strategic Command, and others, as appropriate, to include at a minimum the following information in the fiscal years 2013 through 2015 strategy reports for electronic warfare

- Performance measures to guide implementation of the strategy and help ensure accountability. These could include milestones to track progress toward closing the 34 capability gaps identified by DOD studies.

- Resources and investments necessary to implement the strategy, including those related to key activities, such as developing electronic warfare organizational structures and leadership.

- The parties responsible for implementing the department`s strategy, including specific roles and responsibilities.

-- Direct the Commander of Strategic Command to define the objectives of the Joint Electromagnetic Spectrum Control Center and issue an implementation plan outlining major implementation tasks and timelines to measure progress.

-- Direct the Under Secretary of Defense for Policy, in concert with the Under Secretary of Defense for Acquisition, Technology, and Logistics, as appropriate, to update key departmental guidance regarding electronic warfare--including DOD Directives 3222.4 (Electronic Warfare and Command and Control Warfare Countermeasures) and 3600.01 (Information Operations)--to clearly define oversight roles and responsibilities of and coordination among the Under Secretary of Defense for Policy; the Under Secretary of Defense for Acquisition, Technology, and Logistics; and the Joint Electromagnetic Spectrum Control Center. Additionally, the directives should clarify, as appropriate, the oversight roles and responsibilities for the integration of electronic warfare and cyberspace operations, specifically computer network operations.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD partially concurred with our first recommendation and concurred with our other two recommendations. Regarding our recommendation that DOD include in future strategy reports for electronic warfare, at a minimum, information on (1) performance measures to guide implementation of the strategy, (2) resources and investments necessary to implement the strategy, and (3) parties responsible for implementing the strategy, the department stated that it continues to refine the annual strategy reports for electronic warfare and will expand upon resourcing plans and organization roles; however, the department stated that the strategy was not intended to be prescriptive with performance measures. As we have previously stated, the inclusion of performance measures can aid entities responsible for implementing DOD`s electronic warfare strategy in establishing priorities and milestones to aid in achieving intended results within reasonable time frames. We also have noted that performance measures can enable more effective oversight and accountability as progress toward meeting a strategy`s goals may be measured, thus helping to ensure the strategy`s successful implementation. We therefore continue to believe this recommendation has merit.

DOD concurred with our remaining two recommendations that (1) the Commander of Strategic Command define the objectives of the JEMSCC and issue an implementation plan for the center and (2) DOD update key departmental guidance regarding electronic warfare. These steps, if implemented, will help to clarify the roles and responsibilities of electronic warfare management within the department and aid in the efficient and effective use of resources. DOD`s written comments are reprinted in their entirety appendix III.

We are sending copies of this report to appropriate congressional committees; the Secretary of Defense; and the Commander, U.S. Strategic Command. In addition, this report will be available at no charge on GAO`s web site at [hyperlink, http://www.gao.gov].

If you or your staff have any questions about this report, please contact me at (202) 512-4523 or leporeb@gao.gov Contact points for our offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix IV.

Signed by

Brian J. Lepore Director, Defense Capabilities and Management

Table of Contents

US Urged to Recruit Master Hackers to Wage Cyber War on America's Foes

By Rory Carroll, the Guardian, 10 July 2012

Instead of prosecuting elite computer hackers, the US government should recruit them to launch cyber-attacks against Islamist terrorists and other foes, according to a leading military thinker and government adviser.

The brilliance of hacking experts could be put to use on behalf of the US in the same way as German rocket scientists were enlisted after the second world war, said John Arquilla, a professor of defence analysis at the US Naval Postgraduate School in Monterey, California, in an interview with the Guardian.

He said that the US had fallen behind in the cyber race and needed to set up a "new Bletchley Park" of computer whizzes and codecrackers to detect, track and disrupt enemy networks. "If this was being done, the war on terror would be over," he said.

Arquilla, who invented the term cyberwarfare two decades ago, said a few master hackers had already been recruited but more were needed.

"Let's just say that in some places you find guys with body piercings and non-regulation haircuts. But most of these sorts of guys can't be vetted in the traditional way. We need a new institutional culture that allows us to reach out to them."

Many dabbled in illegal or questionable acts but the US, he noted, had turned Wernher von Braun, Hitler's top scientist, into an American hero after putting him to work on US rockets and space programmes.

Arquilla lambasted lengthy jail terms for hacking, saying it "poisoned" relations between both sides. "It's very, very troubling." He disagreed with the attempt to extradite Gary McKinnon, a British system administrator who has been accused by one US prosecutor of the "biggest military hack of all time" using the code name Solo.

"I think it's ridiculous. They're trying to use deterrences that won't work."

Arquilla, who advised General Norman Schwarzkopf during the first gulf war and secretary of defence Donald Rumsfeld during the second, estimated there were around 100 master hackers in the world, with many, if not most, in Asia and Russia.

He had established contact with several in the US – "they are like shy woodland animals" – and even brought one to meet the CEO of a major company to alert him to his information system's vulnerabilities. The executive, scornful at first, was stunned when the hacker broke into the system with a handheld device in just a few minutes. "All hell broke loose," said Arquilla, who declined to identify the company.

The Pentagon and other security agencies must exploit that sort of ability, he said. "This is huge human capital. They are the rangers of the cyber sphere. Most of them are drawn to it for its beauty and complexity." Few had overt political agendas, but they could be turned into patriots. "Most of the hackers I have known would love to destroy al-Qaida."

Arquilla has long clashed with sceptics who downplay cyber warfare as unproven hype. He said felt vindicated last year when the Pentagon unveiled a new strategy for protecting military computer networks from hackers and designated cyberspace an "operational domain".

The professor was part of a five-member team which advised the Obama administration last year. "Old Higgs had to wait 50 years," he said, referring to the physicist Peter Higgs, whose proposed Higgs boson particle was recently all but confirmed. "I had to wait only 20 years." Last November he published an article titled From Blitzkrieg to Bitskrieg: the military encounter with computers.

The Naval Postgraduate School has close links with the special forces and gives masters and PhD courses to officers from across the services. Arquilla, a contributor to Foreign Policy, is a former director of the Pentagon's Information Operations Center for Excellence. He was also a consultant on the 1995 cyber thriller The Net, starring Sandra Bullock.

The veteran analyst said al-Qaida's loose, decentralised organisational structure had flummoxed the US a decade ago, and that under strategist Abu Musab al-Suri it would become even flatter and looser, impeding traditional counter-terror efforts. The movement, however, was vulnerable. "This global network simply can't thrive without the world wide web and internet. It can't operate without it, or if it does, at a greatly reduced level."

Master hackers, he said, could sabotage their communications. "We must create a new Bletchley Park. Detect, track, disrupt, that's the key. Back-hack so they don't know how we're doing it. And even if we can't do certain things, make them think we can."

Arquilla scorned the state department's admission in May that it had hacked Yemeni tribal websites to change messages about killing Americans as a feeble shadow of what could be done. "If we take the war to them we can win the network war." The Stuxnet worm which attacked Iran's nuclear programme showed the true potential of what he termed "cybotage".

The professor stressed that cyber operations, like air campaigns, could not win wars on their own. Unlike some thinkers he did not fear a major "cyber-Pearl Harbor" attack on the US, saying that the risk was instead small, multiple attacks costing hundreds of billions of dollars.

Hacking, he said, was most effective when incorporated into wider military strategy. The Russians, he said, pioneered this during the August 2008 conflict with Georgia when cyber-attacks sliced through US-designed technology "like a knife through butter", disrupting Georgian forces and paving Russia's quick victory.

Moscow denied mounting cyber operations, and their provenance was never discovered. But Arquilla said "Russian-aligned interests" successfully attacked Estonia's networks during a diplomatic row in 2007. "It's all veiled, but the real leaders in the field are the Russians." China and North Korea were also highly sophisticated. "They understand the strategic uses."

Arquilla compared computer firewalls to the Maginot line – France's failed defence against Germany – and urged US state agencies and companies to use strong encryption and cloud computing to keep data on the move. "The level of insecurity is huge. The average individual is a zombie in some hacker's botnet within half an hour of going online."

He accused the Pentagon and its political masters of wasting billions on pointless aircraft carriers, tanks and planes at the expense of nimbler, leaner strategy. "Militaries often take time to adapt. Think world war one and generals using Waterloo tactics."

Table of Contents

US, Iran Cyber War Beginning

From News24, 13 Jul 2012

A US cyber war against Iran's nuclear programme may have only just begun and could escalate with explosions triggered by digital sabotage, experts say.

Although the Iranian regime remains vulnerable to more cyber attacks in the aftermath of the "Stuxnet" worm that disrupted its uranium enrichment work, Tehran may be receiving help from Russian proxies for its digital security, some analysts say.

The nuclear programme is "really not that well protected" from more digital assaults and Iran will be hard-pressed to safeguard its uranium enrichment efforts from tainted software, said David Albright, president of the Institute for Science and International Security.

"With Stuxnet, they lost about a year. And it caused a lot of confusion. They really didn't know what hit them," he said. "It looks like a viable way to disrupt their programme."

The US, which reportedly masterminded the Stuxnet operation along with Israel, has every incentive to press ahead with a cyber campaign to undermine Iran's atomic ambitions, according to analysts.

Sabotage

The next cyber attack, possibly in combination with more traditional spy craft, could shut off valves or issue incorrect orders that might cause an explosion at a sensitive site.

"I think that it could get more violent," Albright said. "I would expect more facilities to blow up."

A major explosion at a missile plant in Iran in November sparked speculation that the incident was the result of sabotage.

"There is of course the possibility of sending in a team to modify a system in a way that would make it vulnerable, and then use a cyber weapon at a later date as a trigger event," said David Lindahl, research engineer at the Swedish Defence Research Agency.

A new wave of cyber attacks could involve inserting hardware with infected chips into the industrial process, possibly through an agent or a duped employee, or penetrating diagnostic software used to gauge uranium enrichment or other work, Lindahl said.

But some cyber security experts suspect Russian proxies could be assisting Iran with its digital defences, and possibly helped Tehran trace the origins of Stuxnet.

"The part that we probably miscalculated on in Stuxnet was the [possible] assistance of the Russians in attribution," said James Lewis, senior fellow at the Centre for Strategic and International Studies.

"The Iranians never would have figured this out on their own," said Lewis, a former senior government official with the Departments of State and Commerce.

Retaliation

The elaborate Stuxnet malware, which was reportedly introduced using a thumb drive, contained malicious code that caused centrifuges used to enrich uranium to spin out of control. The worm, meanwhile, sent back signals to operators indicating the centrifuges were operating normally.

After the malware was discovered in 2010, at least a thousand centrifuges had to be removed and analysts estimate Tehran's programme was set back by at least a year.

By pushing the boundaries of cyber warfare, the US has left itself open to retaliation. But US officials clearly view the risks associated with digital strikes as dwarfed by the dangers of an all-out war with Iran.

Bombing raids are "more likely to explode the region and certainly could lead to a conflict with Iran, and that would be very messy", said Lewis. "Cyber is much cleaner."

Although unnamed officials told The New York Times that the US and Israel were behind the digital operations, cyber attacks - unlike air strikes - allow for "plausible deniability", he said.

The Stuxnet worm broke new ground by successfully hijacking a programme designed to supervise power plants or other large industrial systems, said Sean McGurk, a consultant who previously led cyber security efforts at the Department of Homeland Security.

Specific target

"Stuxnet demonstrated going from a disruptive capability to a destructive capability and that's what made it unique," he said.

The super virus also was unusual for the way it sought out a specific target while sidestepping systems that did not fit certain criteria.

"Almost all cyber attacks are 'to whom it may concern' but Stuxnet was a bullet with someone's name on it," Lindahl said.

"Repeating something like Stuxnet or [computer virus] Flame will be much more difficult, because they [the Iranians] will spend a lot more energy trying to stop those activities," he added.

"But the defender needs to plug all holes, while the attacker need only find one."

Table of Contents

New Satellites Could Make GPS Harder to Jam

By Lorenzo Franceschi-Bicchierail, WIRED, 25 Jul 2012

Without GPS, drones can’t fly, communications networks can’t function, and you don’t have a chance of figuring out how to get to your Aunt Sadie’s place in New Jersey. And right now, GPS is highly vulnerable because its weak signals are coming from an aging constellation of satellites.

Lockheed Martin, the nation’s biggest military contractor, thinks the next generation of GPS satellites might be able to fix all that. GPS III, as it’s known, is designed to improve the accuracy of the GPS signal and have better resistance to jamming. Also, it is meant to be compatible with its international alternatives like the European Galileo system or the Russian GLONASS system. Potentially, it will improve GPS’ accuracy and resistance to jamming — the deliberate or accidental transmission of radio signals that interfere with regular communications.

In 2008, Lockheed Martin was awarded a $1.4 billion contract to design and develop the system and to build the first two satellites of the new constellation; the first of those is set to be launched in 2014. In January the Air Force gave Lockheed a $238 million contract to produce two more satellites.

Eventually, the Air Force plans to purchase up to 32 satellites that will end up replacing the current constellation of aging GPS satellites. "GPS is really the gold standard internationally for PNT [Position Navigation and Timing]," says Scott Lindell, the director of strategy and business development at Lockheed Martin. "And [it] has become this ubiquitous global utility that everybody is using. Overtime the system needs to be replenished, the satellites on orbit age and at some point they stop working."

Young satellites mean better satellites too. According to Lindell, GPS III will transmit signals eight times as powerful as the current ones, allowing them to have better resistance against jamming. If you think of GPS signals as voices in a noisy room, if you want to be heard, you need to talk louder. That's basically what the new signals will do. With GPS III, "you can tolerate a lot more noise and still be heard," Lindell tells Danger Room.

This improved anti-jamming capabilities will be available both for civilian and military users. "There's better anti-jamming for everybody," says Logan Scott, a GPS industry consultant. And not only the signals will be more powerful, there will be more signals too.

"The mere fact of having more signals available to the civil user is a major improvement in potential security," says Scott, who thinks that could be a potential solution to jamming or even spoofing incidents as a security-conscious GPS receiver — say, one mounted on a civilian drone — could turn to the other satellite signals when it receives one that it doesn't recognize.

But the key is detecting and recognizing it, and that's something that it's not possible today with open, unencrypted and unauthenticated signals like the ones used by civilian GPS. Logan says it's possible to create "marked" signals, so that receivers know they're coming from the satellite instead of some malicious hacker with a spoofer. Problem is, marked signals are not part of GPS III, and it's unclear when or if they will be adopted.

So is GPS III the answer to all GPS troubles? In a word, no. "It would still be vulnerable, it's not enough," says Scott, who thinks the system is still open to attack since there's no backup in case you lose GPS. A radio navigation system called LORAN (LOng RAnge Navigation) was used as backup until January 2010, when it was discontinued by the Department of Homeland Security. Logan considers that a mistake. "LORAN should be re-instituted, if not for navigation at least for timing," he says.

Lindell declined to comment on LORAN, saying Lockheed can't comment on what are ultimately policy decisions for the U.S. government. Meanwhile, the U.S. Air Force has teamed up with Locata, an Australian start-up, to develop an alternative to GPS, at least in limited spaces. Instead of relying on satellites, Locata sets up its own network of Wi-Fi band signal stations, delivering more accurate location data. It's an ideal solution for places where the reach of GPS signals is limited or completely unavailable.

According to Lindell, GPS III will have better accuracy too, which will make the use of GPS possible in hard-to-reach natural areas like canyons or cities, where transmissions are sometimes blocked by skyscrapers – the so-called "urban canyons."

"If you can't see four GPS satellites at one time right now, you will lose accuracy and you could lose the lock on the signal altogether," Lindell tells Danger Room. "In the future you don't have to see four GPS satellites," because apart from the improved power and accuracy of GPS' signals, an average user will be able to take advantage of other systems' satellites. "That allows us to go through urban canyons and real natural canyons.

Lindell declined to estimate when the new constellation of satellites will be in place, saying it's not only up to them. It will depend on the Air Force as well as other factors like the actual need for new satellites since the old ones are still functioning — for now.

Table of Contents

Africa Used As Botnet Army; S E Asia Invests In Information Warfare; Latin America Beefs Up Regulation

From InfoSecurity Magazine, 30 July 2012

At the McAfee office in Silicon Valley, Brian Contos, senior director of emerging markets and vertical solutions, told Infosecurity exactly what the information security landscape is looking like in Africa, South East Asia, and Latin America.

Africa

“Over the last seven to eight years, Africa has become highly connected”, Contos began. “Many of the operating systems in use, however, are pirated, meaning they’re not receiving patches or updates”. As a result of this, Africa is a huge target for hackers to leverage, he explained. “It is being used as a hub to target other countries – using command and control attacks, denial of service, phishing and spam.” His concerns for the future are of a botnet cyber army of over a million. “At the moment, Africa isn’t attacking – they’re being attacked and used”. While businesses in Africa “get security”, Contos does not believe the same can be said of the government and end users. “They aren’t as aware, they’re less secure and they don’t have the money to invest.”

South East Asia

“They know that they can’t win physical wars, so they’re putting muscle behind information warfare”, Contos said of South East Asia. In the small South East Asia countries, there are many university technology graduates, thus a mass of people with the skill-sets required for successful information warfare. “South East Asia is using espionage to improve its level and status in the world. Vietnam could take the UK and US on in a cyberwar”, he insisted. “We know that information warfare is real. What happened in Israel and Syria in 2007 is proof of that.” Contos declared only minimum awareness in governments, claiming “People need more concrete things to happen in order to take it seriously.”

Latin America

While Contos has not seen any cyber terrorist activity in Latin America, he is confident it houses many minor actors and hacktivists. Peru, he advised, is increasing its focus and investment in technology. “It’s becoming a mini Silicon Valley”, he said. “Brazil may have been the first to get online banking, but it was also the first to have it hacked”, Contos remembered. Interestingly, Mexico has evolved from having the “most corrupt online banking system” to the most “heavily regulated in the world”. So regulated and secure, in fact, that people not living in Mexico are moving their money into Mexican banks, Contos announced.

Transcending Geography

Some information security trends transcend geographical borders though, and one of those, Contos advised, is that “we need a carrot.” The information security industry has lots of sticks, he said, referring to financial penalties and bad press. “What we now need is a carrot.”

It is general consensus that the next major war or global conflict will be “owned by the cyber guys”. One of the many reasons for this is that attribution and accountability is very difficult in the cyber space.

The consequence and collateral damage from a cyber war should not be under-estimated, insisted Contos. “If hackers take out the grid – which is vulnerable - there will be a dramatic impact on everything. We are so infrastructure dependent that if water or electricity was cut off, people would start trying to kill each other within two or three days.”

While Contos acknowledges that the information security industry has made great strides in the last five years, so have the cyber criminals. “We’ve had so many new attack vectors and threats thrust upon us”, he said. “Yes, it is possible for defense to get ahead of offense, but to achieve this [the industry] needs to talk to each other”. This is the principle behind the Security Connected initiative at McAfee.

“We need to make security usable. We’ve complicated the hell out of this business”, Contos concluded.

Table of Contents

SOF Electronic Warfare Soldier Works To Save Lives on the Modern Battlefield

By Sgt. Cameron Christensen, Combined Joint Special Operations Task Force – Afghanistan, 23 Jul 2012

KABUL, Afghanistan – As militaries around the world develop new technology to combat the effectiveness of radar and communications, electronic warfare specialists are quickly proving their worth on the frontlines of today’s modern battlefield.

Electronic warfare combats electronic threats; whether they’re from a computer network, satellite system or just ordinary personal devices, like a mobile phone.

“It’s all around us, but you can’t see it,” said Staff Sgt. Eric Rondeau, Combined Joint Special Operations Task Force Afghanistan electronic warfare non-commissioned officer in charge. “And the better we are at controlling the electronic battlefield, the less effective the enemy’s attacks are on us.”

A common electronic warfare attack used today is the remote controlled improvised explosive device. It's a threat that has become closely associated with the war in Afghanistan, and takes the lives of many service members, as well as innocent civilians, every year.

Recently, Rondeau traveled to Camp Integrity in Kabul district, Parwan province, to install two electronic warfare systems on special operations forces vehicles there.

"This system, known as Egon, is a highly effective piece of equipment for protection against remote-controlled IEDs," said Rondeau. "It's SOF's version of the conventional forces RC-IED jammer, and it will protect them."

Since April, there have been 15 known incidents of failed RC-IEDs in Afghanistan directly attributed to the EGON system, according to Maj. Greg Wells, CJSOTF-A electronic warfare officer.

"In one instance, SOF operators reported halting their vehicles during a convoy. As they began clearing the immediate area, they found an RC-IED under one of the tires of a vehicle in the convoy," said Wells. "Proof the Egon system works."

Electronic warfare isn't limited to just combating RC-IEDs. It encompasses the attack and defense of all electronic networks and communications systems, like GPS and satellite communications.

"They call me the 'jammer guy,'" said Rondeau. "So, I'm trying to educate people about EW, because there's a misunderstanding about it. I'm not just the 'jammer guy,' and that's why I try to train as I travel."

Through on-the-spot training, given during his frequent visits to more than one hundred special operations forces sites, he informs the special operations forces operators who rely daily on electronic warfare equipment, like the Egon, to keep them safe.

"The more they understand, the more apt they are to use the equipment," said Rondeau. "Bottomline, this job saves lives."

Table of Contents

Hackers Linked to China's Army Seen From EU to D.C.

By Michael Riley and Dune Lawrence, Bloomberg News, Jul 26, 2012

The hackers clocked in at precisely 9:23 a.m. Brussels time on July 18 last year, and set to their task. In just 14 minutes of quick keyboard work, they scooped up the e-mails of the president of the European Union Council, Herman Van Rompuy, Europe's point man for shepherding the delicate politics of the bailout for Greece, according to a computer record of the hackers' activity.

Over 10 days last July, the hackers returned to the council's computers four times, accessing the internal communications of 11 of the EU's economic, security and foreign affairs officials. The breach, unreported until now, potentially gave the intruders an unvarnished view of the financial crisis gripping Europe.

And the spies were themselves being watched. Working together in secret, some 30 North American private security researchers were tracking one of the biggest and busiest hacking groups in China.

Observed for years by U.S. intelligence, which dubbed it Byzantine Candor, the team of hackers also is known in security circles as the Comment group for its trademark of infiltrating computers using hidden webpage computer code known as "comments."

During almost two months of monitoring last year, the researchers say they were struck by the sheer scale of the hackers' work as data bled from one victim after the next: from oilfield services leader Halliburton Co. (HAL) to Washington law firm Wiley Rein LLP; from a Canadian magistrate involved in a sensitive China extradition case to Kolkata-based tobacco and technology conglomerate ITC Ltd. (ITC)

Gathering Secrets

The researchers identified 20 victims in all -- many of them organizations with secrets that could give China an edge as it strives to become the world's largest economy. The targets included lawyers pursuing trade claims against the country's exporters and an energy company preparing to drill in waters China claims as its own.

"What the general public hears about -- stolen credit card numbers, somebody hacked LinkedIn (LNKD) -- that's the tip of the iceberg, the unclassified stuff," said Shawn Henry, former executive assistant director of the FBI in charge of the agency's cyber division until leaving earlier this year. "I've been circling the iceberg in a submarine. This is the biggest vacuuming up of U.S. proprietary data that we've ever seen. It's a machine."

Exploiting a hole in the hackers' security, the researchers created a digital diary, logging the intruders' every move as they crept into networks, shut off anti-virus systems, camouflaged themselves as system administrators and covered their tracks, making them almost immune to detection by their victims.

Every Move

The minute-by-minute accounts spin a never-before told story of the workaday routines and relentless onslaught of a group so successful that a cyber unit within the Air Force's Office of Special Investigations in San Antonio is dedicated to tracking it, according to a person familiar with the unit.

Those logs -- a record of the hackers' commands to their victims' computers -- also reveal the highly organized effort behind a group that more than any other is believed to be at the spear point of the vast hacking industry in China. Byzantine Candor is linked to China's military, the People's Liberation Army, according to a 2008 diplomatic cable released by WikiLeaks. Two former intelligence officials verified the substance of the document.

Hackers and Spies

The methods behind China-based looting of technology and data -- and most of the victims -- have remained for more than a decade in the murky world of hackers and spies, fully known in the U.S. only to a small community of investigators with classified clearances.

"Until we can have this conversation in a transparent way, we are going to be hard pressed to solve the problem," said Amit Yoran, former National Cyber Security Division director at the Department of Homeland Security.

Yoran now works for RSA Security Inc., a Bedford, Massachusetts-based security company which was hacked by Chinese teams last year. "I'm just not sure America is ready for that," he said.

What started as assaults on military and defense contractors has widened into a rash of attacks from which no corporate entity is safe, say U.S. intelligence officials, who are raising the alarm in increasingly dire terms.

In an essay in the Wall Street Journal July 19, President Barack Obama warned that "the cyber threat to our nation is one of the most serious economic and national security challenges we face." Ten days earlier, in a speech given in Washington, National Security Agency director Keith Alexander said cyber espionage constitutes "the greatest transfer of wealth in history," and cited a figure of $1 trillion spent globally every year by companies trying to protect themselves.

Harvesting Secrets

The networks of major oil companies have been harvested for seismic maps charting oil reserves; patent law firms for their clients' trade secrets; and investment banks for market analysis that might impact the global ventures of state-owned companies, according to computer security experts who asked not to be named and declined to give more details.

China's foreign ministry in Beijing has previously dismissed allegations of state-sponsored cyberspying as baseless and said the government would crack down if incidents came to light. Contacted for this story, it did so again, referring to earlier ministry statements.

Private researchers have identified 10 to 20 Chinese hacking groups but said they vary significantly in activity and size, according to government investigators and security firms.

Group Apart

What sets the Comment group apart is the frenetic pace of its operations. The attacks documented last summer represent a fragment of the Comment group's conquests, which stretch back at least to 2002, according to incident reports and interviews with investigators. Milpitas, California-based FireEye Inc. alone has tracked hundreds of victims in the last three years and estimates the group has hacked more than 1,000 organizations, said Alex Lanstein, a senior security researcher.

Stolen information is flowing out of the networks of law firms, investment banks, oil companies, drug makers, and high technology manufacturers in such significant quantities that intelligence officials now say it could cause long-term harm to U.S. and European economies.

'Earthquake Is Coming'

"The activity we're seeing now is the tremor, but the earthquake is coming," said Ray Mislock, who before retiring in September was chief security officer for DuPont Co., which has been hacked by unidentified Chinese teams at least twice since 2009.

"A successful company can't sustain a long-term loss of knowledge that creates economic power," he said.

Even those offline aren't safe. Y.C. Deveshwar, 65, a businessman who heads ITC, India's largest maker of cigarettes, doesn't use a computer. The Comment hackers last year still managed to steal a trove of his documents, navigating the conglomerate's huge network to pinpoint the machine used by Deveshwar's personal assistant.

On July 5, 2011, the thieves accessed a list of documents that included Deveshwar's family addresses, tax filings, and meeting minutes, as well as letters to fellow executives, such as London-based British American Tobacco Plc (BATS) chairman Richard Burrows and BAT chief executive, Nicandro Durante, according to the logs. They tried to open one entitled "YCD LETTERS" but couldn't, so the hackers set up a program to steal a password the next time his assistant signed on.

Keeping Quiet

When Bloomberg contacted the company in May, spokesman Nazeeb Arif said ITC was unaware of the breach, potentially giving the hackers unimpeded access to ITC's network for more than a year. Deveshwar said in a statement that "no classified company related documents" were kept on the computer.

Companies that discover their networks have been commandeered usually keep quiet, leaving the public, shareholders and clients unaware of the magnitude of the problem. Of the 10 Comment group victims reached by Bloomberg, those who learned of the hacks chose not to disclose them publicly, and three said they were unaware they'd been hacked until contacted for this story.

This account of the Comment group is based on the researchers' logs, as well as interviews with current and former intelligence officials, victims, and more than a dozen U.S. cybersecurity experts, many of whom track the group independently.

Private Investigators

The researcher who provided the computer logs asked not to be named because of the sensitivity of the data, which included the name of victims. He was part of a collaborative drawn from 20 organizations that included people from private security companies, a university, internet service providers and companies that have been targeted, including a defense contractor and a pharmaceutical firm. The group included some of the top experts in the field, with experience investigating cyberspying against the U.S. government, major corporations and high profile political targets, including the Dalai Lama.

Like similar, ad hoc teams formed temporarily to study hackers' techniques, the group worked in secret because of the sensitivities of the investigation aimed at state-sponsored espionage. A smaller version of the group is continuing its research.

As the surge in attacks on businesses and non-government groups over the last five years has pulled private security experts into the hacker hunt, they say they're gradually catching up with U.S. counterintelligence agencies, which have been tackling the problem for a decade.

Espionage Tools

One Comment group trademark involves hijacking unassuming public websites to send commands to victim computers, turning mom-and-pop sites into tools of foreign espionage, but also allowing the group to be monitored if those websites can be found, according to security experts. Sites it has commandeered include one for a teacher at a south Texas high school with the website motto "Computers Rock!" and another for a drag racing track outside Boise, Idaho.

Adding a potentially important piece to the puzzle, researcher Joe Stewart, who works for Dell SecureWorks, an Atlanta-based security firm and division of Dell Inc. (DELL), the computer technology company, last year uncovered a flaw in software used by Comment group hackers. Designed to disguise the pilfered data's ultimate destination, the mistake instead revealed that in hundreds of instances, data was sent to Internet Protocol (IP) addresses in Shanghai.

Military Link?

The location matched intelligence contained in the 2008 State Department cable published by WikiLeaks that placed the group in Shanghai and linked it to China's military. Commercial researchers have yet to make that connection. The basis for that cable's conclusion, which includes the U.S.'s own spying, remains classified, according to two former intelligence specialists.

Lanstein said that although the make-up of the Comment group has changed over time -- the logs show some inexperienced hackers in the group making repeated mistakes, for example --the characteristics of a single group are unmistakable. The code and tools used by Comment aren't public, and anyone using it would have to be given entre into the hackers' ranks, he said.

By October 2008, when the diplomatic cable published by WikiLeaks outlined the group's activities, the Comment group had raided the networks of defense contractors and the Department of State, as well as made a specialty of hacking U.S. Army systems. The classified code names for China's hacking teams were changed last year after that leak.

Cybersecurity experts have connected the group to a series of headline-grabbing hacks, ranging from the 2008 presidential campaigns of Barack Obama and John McCain to the 72 victims documented last year by the Santa Clara, California-based security firm McAfee Inc., in what it called Operation Shady Rat.

Nuclear Break-In

Others, not publicly attributed to the group before, include a campaign against North American natural gas producers that began in December 2011 and was detailed in an April alert by the Department of Homeland Security, two experts who analyzed the attack said. In another case, the hackers first stole a contact list for subscribers to a nuclear management newsletter, and then sent them forged e-mails laden with spyware.

In that instance, the group succeeded in breaking into the computer network of at least one facility, Diablo Canyon nuclear plant, next to the Hosgri fault north of Santa Barbara, according to a person familiar with the case who asked not to be named.

Last August, the plant's incident management team saw an anonymous Internet post that had been making the rounds among cybersecurity professionals. It purported to identify web domains being used by a Chinese hacking group, including one that suggested a possible connection to Diablo plant operator Pacific Gas & Electric Co., according to an internal report obtained by Bloomberg News.

Partial Control

It's unclear how the information got to the Internet, but when the plant investigated, it found that the computer of a senior nuclear planner was at least partly under the control of the hackers, according to the report. The internal probe warned that the hackers were attempting "to identify the operations, organizations, and security of U.S. nuclear power generation facilities."

The investigators concluded that they had caught the breach early and there was "no solid indication" data was stolen, according to the report, though they also found evidence of several previous infections.

Blair Jones, a spokesman for PG&E, declined to comment, citing plant security.

Around the time the hackers were sending malware-laden e- mails to U.S. nuclear facilities, six people at the Wiley Rein law firm were ushered into hastily called meetings. In the room were an ethics compliance officer and a person from the firm's information technology team, according to a person familiar with the investigation. The firm had been hacked, each of the six were told, and they were the targets.

Lawyers' Files

Among them were Alan Price and Timothy Brightbill. Firm partners and among the best known international trade lawyers in the country, they've handled a series of major anti-dumping and unfair trade cases against China. One of those, against China's solar cell manufacturers, in May resulted in tariffs on more than $3 billion in Chinese exports, making it one of the largest anti-dumping cases in U.S. history.

Dale Hausman, Wiley Rein's general counsel, said he couldn't comment on how the breach affected the firm or its clients. Wiley Rein has since strengthened its network security, Hausman said.

"Given the nature of that practice, it's almost a cost of doing business. It's not a surprise," he said.

E-Mails to Spouses

Tipped off by the researchers, the firm called the Federal Bureau of Investigation, which dispatched a team of cyber investigators, the person familiar with the investigation said. Comment hackers had encrypted the data it stole, a trick designed to make it harder to determine what was taken. The FBI managed to decode it.

The data included thousands of pages of e-mails and documents, from lawyers' personal chatter with their spouses to confidential communications with clients. Printed out in a stack, the cache was taller than a set of encyclopedias, the person said.

Researchers watching the hackers' keystrokes last summer say they couldn't see most of what was stolen, but it was clear that the spies had complete control over the firm's e-mail system. The logs also hold a clue to how the FBI might have decrypted what was stolen. They show the simple password the hackers used to encrypt the files: 123!@#. Paul Bresson, a spokesman for the FBI in Washington, declined to comment.

Following the Crisis

In case after case, the hackers' trail crisscrossed with geopolitical events and global headlines. Last summer, as the news focused on Europe's financial crisis, with its import for China's rising economic power, the hackers followed.

The timing coincided with an intense period for EU Council President Van Rompuy, set off by the failure July 11 of the EU finance ministers to agree on a second bailout package for Greece. Over the next 10 days, the slight and balding former Belgian prime minister presided over the negotiations, drawing European leaders, including German Chancellor Angela Merkel, to a consensus.

Although the monitoring of Van Rompuy and his staff occurred during those talks, researchers say that the logs suggest a broad attack that wasn't timed to a specific event. It was the cyber equivalent of a wiretap, they say -- an operation aimed at gathering vast amounts of intelligence over weeks, perhaps months.

'Big Implications'

Richard Falkenrath, former deputy homeland security adviser to President George W. Bush, said China has succeeded in integrating decision-making about foreign economic and investment policy with intelligence collection.

"That has big implications for the rest of the world when it deals with the country on those terms," he said.

Beginning July 8, 2011, the hackers' access already established, they dipped into the council's networks repeatedly over 10 days. The logs suggest an established routine, with the spies always checking in around 9 a.m. local time. They controlled the council's exchange server, which gave them complete run of the e-mail system, the logs show. From there, the hackers simply opened the accounts of Van Rompuy and the others.

Week of E-Mails

Moving from one victim to the next, the spies grabbed e- mails and attached documents, encrypted them in compression files and catalogued the reams of material by date. They grabbed a week's worth of e-mails each time, appearing to follow a set protocol. Their other targets included then economic adviser and deputy head of cabinet, Odile Renaud-Basso, and the EU's counter-terrorism coordinator. It's unclear how long the hackers had been in the council's network before the researchers' monitoring began -- or how long it lasted after the end of July last year.

There's no indication the hackers penetrated the council's offline system for secret documents. "Classified information and other sensitive internal information is handled on separate, dedicated networks," the council press office said in a statement when asked about the hacks. The networks connected to the Internet, which handle e-mail, "are not designed for handling classified information."

What the EU did about the breach is unclear. Dirk De Backer, a spokesman for Van Rompuy, declined to comment on the incident, as did an official from the EU Council's press office. A member of the EU's security team joined the group of researchers in late July, and was provided information that would help identify the hackers' trail, one of the researchers said.

"No Knowledge"

Zoltan Martinusz, then principal adviser on external affairs and one of two victims reached by Bloomberg who would address the issue, said, "I have no knowledge of this." The other official, who wasn't authorized to discuss internal security and asked not to be identified, said he was informed last year that his e-mails had been accessed.

The logs show how the hackers consistently applied the same, simple line of attack, the researchers said. Starting with a malware-laden e-mail, they moved rapidly through networks, grabbing encrypted passwords, cracking the coding offline, and then returning to mimic the organization's own network administrators. The hackers were able to dip in and out of networks sometimes over months.

The approach circumvented the millions of dollars the organizations collectively spent on protection.

Security Switched Off

As the spies rifled the network of Business Executives for National Security Inc., a Washington-based nonprofit whose advisory council includes former Secretary of State Henry Kissinger and former Treasury Secretary Robert Rubin, the logs show them switching off the system's Symantec anti-virus software. Henry Hinton Jr., the group's chief operations officer, said in June he was unaware of the hack, confirming the user names of staff computers that the logs show were accessed, his among them.

The records show the hackers' mistakes, but also clever tricks. Using network administrator status, they consolidated onto a single machine the computer contents of the president and seven other staff members of the International Republican Institute, a nonprofit group promoting democracy.

220 Documents

With all that data in one place, the hackers on June 29, 2011, selected 220 documents, including PDFs, spreadsheets, photos and the organization's entire work plan for China. When they were done, the Comment group zipped up the documents into several encrypted files, making the data less noticeable as it left the network, the logs show.

Lisa Gates, a spokeswoman for the IRI, confirmed that her organization was hacked but declined to comment on the impact on its programs in China because of concern for the safety of staff and people who work with the group. A funding document describes activities including supporting independent candidates in China, who frequently face harassment by China's authorities.

As a portrait of the hackers at work, the logs also show how nimbly they could respond to events, even when sensitive government networks were involved. The hackers accessed the network of the Immigration and Refugee Board of Canada July 18 last year, targeting the computer of Leeann King, an immigration adjudicator in Vancouver.

King had made headlines less than a week earlier when she temporarily freed Chinese national Lai Changxing in the final days of a long extradition fight. Chinese authorities had been chasing Lai since he fled to Canada in 1999, alleging that he ran a smuggling ring that netted billions of dollars.

Cracking Court Accounts

Monitoring by Cyber Squared Inc., an Arlington, Virginia- based company that tracks Comment independently and that captured some of the same activity as the researchers, recorded the hackers as they worked rapidly to break into King's account. Beginning only with access to computers in Toronto, the hackers grabbed and decrypted user passwords, gaining access to IRB's network in Vancouver and ultimately, the logs show, to King's computer. From start to finish, the work took just under five hours.

Melissa Anderson, a spokeswoman for the board, said officials had no comment on the incident other than to say that any such event would be fully investigated. Lai was eventually sent back to China on July 23, 2011 after losing a final appeal. He was arrested, tried, and in May of this year, a Chinese court sentenced him to life in prison.

Controlling the Networks

In case after case, the hackers had the run of the networks they were rifling. It's unclear how many of the organizations researchers contacted, but in only one of those cases was the victim already aware of the intrusion, according to one member of the group. Halliburton officials said they were aware of the intrusion and were working with the FBI, one of the researchers said.

Marisol Espinosa, a spokeswoman for the publicly traded company, declined to comment on the incident.

The trail last summer led to some unlikely spots, including Pietro's, an Italian restaurant a couple of blocks from Grand Central station in New York. In business since 1932, guests to the dim, old-fashioned dining room can choose linguine with clam sauce (red or white) for $28. The Comment group stopped using the restaurant's site to communicate with hacked networks sometime last year, said FireEye's Lanstein, who discovered that the hackers had left footprints there. Traces are still there.

’Ugly Gorilla’

Hidden in the webpage code of the restaurant's site is a single command: ugs12, he said. It's an order to a captive computer on some victim's network to sleep for 12 minutes, then check back in, he explained. The ”ug” stands for “ugly gorilla,” what security experts believe is a moniker for a particularly brash member of Comment, a signal for anyone looking that the hackers were there, said Lanstein.

“We're so good even hackers want us!” joked Bill Bruckman, the restaurant's co-owner, when he was told his website had been part of the global infrastructure of a Chinese hacking team. “Hey, put my name out there -- any business is good business,” he said.

Bruckman said he knew nothing about the breach. A few friends reported trouble accessing the site about six months ago, though he said he'd never figured out what the problem was.

Outside a moment later, smoking a cigarette, Bruckman added a more serious note.

“Think of all that effort and information going down the drain. What a waste, you know what I mean?”

Table of Contents

A Computer Infection that Can Never Be Cured

By Tom Simonite, Technology Review, 1 Aug 2012

As the manufacturing of computers and other gadgets has migrated to China, an occasional paranoid voice has asked whether the country might be tempted to preinstall software for surveillance. This remains a far-fetched notion, but now a French hacker has at least shown how such a covert back door could be created.

At the Black Hat security conference in Las Vegas last week, Jonathan Brossard demonstrated software that can be hidden deep inside the hardware of a PC, creating a back door that would allow secret remote access over the Internet. His secret entrance can't even be closed by switching a PC's hard disk or reinstalling its operating system.

Corporate and government-sponsored computer espionage is a growing problem, and hackers are using ever more sophisticated methods to bypass security ramparts. A congressional report, published in March this year, concluded that electronics manufactured in China posed a "potential" threat to U.S. communication systems, but there is no evidence of attempted espionage by hiding surveillance tools inside new equipment to date.

Brossard's backdoor tool, dubbed Rakshasa, needs to be installed into the BIOS chip on a PC's motherboard, on which the main processor and other core components are mounted. A computer's BIOS chip contains the first code, known as firmware, which a computer runs when it is powered on to start the process of booting up the operating system. Brossard also found he could hide his malicious code inside chips of other hardware components such as network cards, and have it jump into the BIOS when necessary.

"If someone puts a single rogue firmware on your machine, he basically owns you forever," Brossard told an audience of fellow hackers and computer security professionals at Black Hat.

When a PC with Rakshasa installed is switched on, the software looks for an Internet connection to fetch the small amount of code it needs to compromise the computer. If Rakshasa can't get an Internet connection, it can't operate.

The design makes Rakshasa extra stealthy. "For a nation-state-quality back door, think Flame or Stuxnet, we want plausible deniability," explained Brossard, referring to malware that experts believe was created by government-sponsored hackers. "If you fetch over the Internet every time, we don't leave a trace on the file system."

The code Rakshasa fetches is used to disable a series of security controls that limit what changes low-level code can make to the high-level operating system and memory of a computer. Then, as the computer's operating system is booted up, Rakshasa uses the powers it has granted itself to inject code into key parts of the operating system. Such code can be used to disable user controls, or steal passwords and other data to send back to the person controlling Rakshasa.

In an onstage demonstration at Black Hat, Brossard proved his idea works by having Rakshasa boot a computer with Windows 7 installed and override its password authentication. A person chosen from the audience was then able to use a randomly chosen password to log into the admin account.

Brossard built Rakshasa by combining several legitimate open-source software packages for altering firmware. Due to the efforts of programmers that have contributed to those projects, Rakshasa works on 230 different models of motherboard, says Brossard. It likely works on many more models of PC, since it is common for a manufacturer to use the same motherboard model in many different PC models.

Because Rakshasa only ever resides inside motherboard chips, it is safely out of view of antivirus software and resilient to the most common responses by IT staff cleaning up a badly infected PC.

"Even if you change your hard drive or change your OS, you're still very much going to be owned," said Brossard, who has tested the code that Rakshasa fetches against a standard battery of 43 antivirus programs and found that none flagged it as dangerous.

Of course, deploying Rakshasa would require getting access to the motherboard of a computer, perhaps in a factory or warehouse. "Another attack scenario is you buy a new network card and get back-doored," said Brossard, because of the way Rakshasa can jump from other components into the BIOS.

Anyone fearing a Rakshasa-style attack would need to replace the firmware on the chips of the motherboard and other components with versions known to be safe.

The attack can work on PCs with any kind of processor, but many of the standard features of PC motherboards originated with Intel. Suzy Greenberg, a spokeswoman for that company, said in an e-mail that Brossard's paper was "largely theoretical," since it did not specify how an attacker would insert Rakshasa onto a system, and did not take into account that many new BIOS chips have cryptographically verified code that would prevent it from working.

However, Brossard notes that this added layer of protection is available only on a minority of PCs so far, and that an organization with access to PC manufacturing or distribution would have many opportunities to install Rakshasa-style software.

Table of Contents

DECEPTION: Can Information Superiority Be Achieved With Or Without It?

By John M. Roach, Newsletter of the OPSEC Professionals Society, July 2012, vol 3, issue 2

Technological innovation and the capacity to manipulate information for specific battlefield effects have become essential to waging modern warfare and underlie themes related to information superiority. However, achieving information superiority will be difficult, if not impossible due to a great number of issues, not the least of which will be an adversary's ability, or ours for that matter, to successfully employ denial and deception (D&D) capabilities.[1]

The nature of deception is to cause another to believe what is not true with the intent to influence their behavior. At face value, deception can be considered quite immoral and socially improper within many cultures. However, the use of deception as a warfighting practice - other than perfidy and treachery - has been the exception to social norms and dates back as early as Sun Tzu, who stated in the Art of War, "All war is based on deception."[2] In short, the nature of deception, void of any moral or ethical judgment, operates with two criteria; first it is intentional; and second, it is designed to gain an advantage for the practitioner.[3] Applied to military operations, deception creates two effects within the battle spaces, those being security and surprise and is among the least expensive military activities in terms of forces and assets to achieve these effects.[4]

Deception, admittedly played only an informal part on the battlefield throughout history, confined mostly at the tactical and more rarely at the operational level until the twentieth century when it was doctrinally embraced and thrust further up to the strategic level. The adaptation of D&D in Western military strategic thought during the 20th Century parallels the growth in the importance of intelligence to national security during the same period. As detection and monitoring systems underwent vast improvements coupled with the explosion in information technology, it reinforced the need for D&D capabilities.

Most recently US Air Force doctrine (2005) discusses "influence operations" as one of the four major components of the information environment which includes psychological operations, military deception, operations security, counter-intelligence, public affairs and counter-propaganda. All of these concepts have the same aim, that is, to influence the mind and behavior of the adversary. To practice any of these would require coordination of D&D to some greater or lesser degree.

Deception used as a broad, general term includes the elements of both denial and deception, each having distinct actions that are either active or passive. Active deception involves providing an adversary with evidence of intentions and capabilities you do not in fact possess. In other words showing an adversary something that is not real.[5] Denial, or passive deception, on the other hand, is designed to hide real intentions or something that really exists. A unique aspect of the relationship between denial and deception is that denial does not need to involve or incorporate active deception to be successful. However, deception must include passive deception to hide reality while developing a false picture for the adversary.

Drawing from American joint doctrine, in the absence of similar Canadian or NATO doctrine, Military Deception (MILDEC) is defined as actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.[6] Operations Security (OPSEC), a form of passive deception, is defined as a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to a) Identify those actions that can be observed by adversary intelligence systems; b) Determine what indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.[7]

Deception at the strategic level is planned and executed by national, alliance or coalitional level authorities, both in peace and war, encompassing measures from political, diplomatic and informational.[8] The assumption that must be made with regard to alliance or coalitional military operations is that deception would be limited to denial to avoid any political or social sensitivity associated with active deception techniques. At the operational level, deception pertains to military actions and measures to deceive an enemy as to time, place and details of planned major operations conducted as part of a campaign or major joint or combined operations with a strategic objective.[9] Tactical deception is intended to mislead opposing actical commanders in terms of time, space, capabilities and intentions of tactical actions.

The adversary decision-maker is always the target of deception whether OPSEC or MILDEC. To reach them, vulnerabilities in the adversary intelligence process must be exploited. Historically, a majority of intelligence analysts receive little training in foreign deception techniques, impeding their ability to detect foreign D&D operations.[10] Even if an analyst does consider foreign D&D to be in play, the tendency is to explain or discount their own cognitive dissonance in a form of self-denial as a result of not fully understanding the role culture plays in D&D operations. Denial is aimed at the collection phase of the intelligence cycle, denying the intelligence analyst key bits of information on which to base assessments. Deception is aimed at the processing phase of the intelligence cycle, relying on denial to cover reality, while false or misleading information is directed at the analyst, which will elicit an improper assessment from the analyst that will support friendly forces intentions.

Other perspectives on D&D include Maskirovka, a concept developed in the former Soviet Union. Maskirovka is considered a set of processes employed during the soviet era designed to mislead, confuse and interfere with anyone accurately assessing its plans objectives, strengths and weaknesses. Denial and deception where not treated as separate activities. The Soviet concept included, but was not limited to deception, disinformation, secrecy and security.[11] Maskirovka was to contribute to the achievement of surprise for the actions of forces, the preservation of combat readiness and the increased survivability of objectives.[12] Highlighting the cultural undertones associated with Maskirovka, "The Soviet experience imparted a culture of deceit…particularly on the military. Lying routinely occurs at the most senior uniformed levels, even when an argument is clearly untenable or contradicted by obvious facts."[13]

Akin to western military doctrine, theological doctrines often turn operational within the Islamic school of thought, for example as in the interpretation and utilization of taqiyya (pronounced *tark-e-ya*) and kitman from the Qur'an. Early Muslim warriors believed their very manhood rested on chivalrous, generous, hospitable and consistently honourable behaviour.[14] Like other warrior codes of honour, D&D was viewed as an unacceptable way of fighting. However, in al-Bukhari, Chapter 73, hadith No. 1298, Muhammad said, "Verily, war is deception."[15] Muslim scholars would debate the use of dissimulation and concluded that deception was sanctioned to win wars but should not operate in daily social life.[16]

The Islamic tradition of taqiyya originated in the sixth- century A.D. following disputes over succession after the Prophet Mohammed's death. The minority Shi'ite developed taqiyya to conceal true beliefs from the Sunni majority and to maintain operations security for jihad operations.[17] Taqiyya is a form of deception intended to cover true feelings. It is lying with the tongue only and not the heart. As such, taqiyya can equate to active deception techniques. Passive Islamic deception would be kitman. Kitman comes from the word katama, which means, to hide or conceal. It is important to realize that it is a form of trust. Kitman is concealing or keeping parts of the whole truth secret. "Kitman may extend to cover the secrets of the whole state at the time of war and peace where a person who is loyal to his people can not divulge to anyone or tell the enemy about his countries afters."[18] The concept of kitman is not unlike the western security concept of the need-to-know principle.

Countering D&D begins with understanding that anyone can be denied or deceived and while we may find the idea of deception distasteful, there are varying degrees of its acceptance within different cultures and religions, not least of which is the legal use of ruses within the Geneva Conventions. Once we have accepted the fact that we can be deceived, author Major Brian Cyr, USMC, Foreign Denial and Deception: Minimizing the Impact to Operational Intelligence, advocates three lines of operation in developing a counter-deception capability.[19] The first line of operation is training and awareness, noting that while most military institutions address operational deception and planning, few touch upon foreign OPSEC aspects of deception. His second line of operation suggests an all source collection and analysis approach. "It is through a variety of channels or collection means, that the J2 increases his ability to detect incongruities in an opponent's D&D cover story. A major reason for this is that the enemy might not have been consistent in portraying his cover story among all channels of information available to him."[20] Finally, it is important that human factors are not ignored. Operators and intelligence analysts must be able to know an adversary and think like them. In order to do this they must be open to evidence that does not fit their own preconceptions and biases.[21] In other words, we have to become more culturally aware of others and how they see the world both through secular and religious lenses to identify foreign D&D.

Despite continuing revolutions in military affairs, modernization, digitalization, transformation or any other evolutionary processes, there are a few things that have remained constant within warfare. Lying is one of them. Denial and deception have centuries old culturally diverse historical roots tied to the principles of warfighting. As methods of information collection have improved, become user friendly and ubiquitous, D&D has not disappeared; rather it has grown in importance and something that requires more attention. Focusing on a national D&D capability is just a starting point. There will be bigger challenges in how to conduct D&D within alliances like NATO or organizations like the United Nations.

In the end, deception in warfare is about limiting access to the whole truth or altering the truth completely and being able change behavior because of it. No matter how sophisticated modern warfare it will be, deception will continue to have a place in it. The inability of technologically advance nations to completely negate the effects of deception, which are often cheap and cost effective, makes deception an effective part of asymmetrical strategies. If information superiority is a key component of future military strategies, then the ability to employ and detect deception will play a large role in its attainment or prevention.

Notes

[1] Lasley, Jennifer. Denial and Deception: A serious threat to Information Superiority. National Defence University, 19 April 2000. Pg. 2

[2] Perfidy was part of the customary laws of war long before the prohibition of perfidy was included in 1977 Protocol I Additional to the Geneva Conventions of 12 August 1949

[3] Caddell, Joseph. Deception 101 – Primer on Deception, US Army War College, Dec 2004, pg.1

[4] Vego, Milan. Operational Deception in the Information Age. Joint Forces Quarterly, Spring 2002, pg. 60

[5] Cadell, pg. 6

[6] While the CF Land Forces Information Operations publication series includes doctrine on Deception, it is limited to tactical deception and is drawn largely from US Army Doctrine. Canada does not have doctrine on OPSEC.

[7] US DoD. JP-3-13 – Joint Doctrine for Operations Security, 2006.

[8] Vego, pg. 62.

[9] Ibid

[10] Lasley, pg. 6

[11] Shea, Tim, LCol. Post-Soviet Maskirovka, Cold War Nostalgia and Peacetime Engagement. Military Review, May-June 2002, pg.63

[12] Yefrimov YA and Chermashentsev, Maskirovka, Soviet Military Encyclopedia, Vol 5, Moscow, Voyenizdat, 1978, pg. 175-177

[13] Shea, pg. 64

[14] Youssef, H. Aboul-Enein, Zuhur, Sherifa. Islamic Rulings on Warfare. US Army War College. October 2004. Pg. 25

[15] Ibid

[16] Ibid

[17] Campbell, Andrew. Taqiyya: How Islamic extremists deceive the West. National Observer, 22 Dec 2005.

[18] Ahmad Sa'd, Islam Online.net, The Islamic perspective of Concealing, 06 Nov 2003. http://www.islamonline.net

[19] Cyr, Brian Maj. USMC. Foreign Denial and Deception: Minimizing the Impact to Operational Intelligence. Naval War College, February 2002.

[20] Ibid, pg. 10

[21] Ibid, pg.12

Table of Contents